

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007216

(43)Date of publication of application : 11.01.2002

(51)Int.Cl.

G06F 12/14

G06F 3/06

(21)Application number : 2000-
191749

(71)Applicant : NEC GUMMA LTD

(22)Date of filing :

26.06.2000

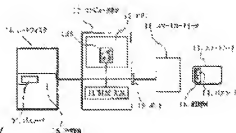
(72)Inventor : SATO SACHIKO

(54) SECURITY SYSTEM OF HARD DISK DRIVE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a security system of a hard disk drive which disables a third person can readily cancel the security of.

SOLUTION: This is the security system of the hard disk drive as a storage device of a computer system and comprises a card-type memory device 17, which stores security data D1 and security data D2 stored on the hard disk drive 14, a card reader 16 which reads out the security data D2 stored in the card type memory device 17, and a comparison means 12A which compares the D1 and D2; when the comparison means 12A detects the security data D1 stored on the hard disk drive 14 which is the same as the security data D2 stored in the card-type memory device 17, the hard disk drive 14 is set in a usable state.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許公開公開番号

特開2002-7216

(P2002-7216A)

(43) 公開日 平成14年1月11日 (2002.1.11)

(51) Int. Cl. ⁷	識別記号	F I	特-7216*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 H 5 B 0 6 5

審査請求 未請求 請求項の数 3 ○ L (全 5 頁)

(21) 出願番号 特願2000-191749 (P2000-191749)

(22) 出願日 平成12年6月26日 (2000.6.26)

(71) 出願人 060165033

群馬日本電気株式会社

群馬県太田市西矢島町32番地

(72) 発明者 佐藤 将子

群馬県太田市西矢島町32番地 群馬日本電

気株式会社内

(74) 代理人 100070530

弁理士 畑 義之

Fターム(参考) 5B017 A03 B09 BB10 CM7

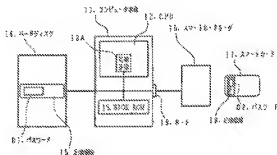
5B065 BA01 PA04 PA15

(54) 【発明の名称】 ハードディスク装置のセキュリティシステム

(57) 【要約】 (修正有)

【課題】 第三者が簡単にセキュリティの解除を行えないようにしたハードディスク装置のセキュリティシステムを提供する。

【解決手段】 コンピュータ装置の記憶装置であるハードディスク装置のセキュリティシステムであって、前記ハードディスク装置14内に格納したセキュリティデータD1と、セキュリティデータD2を格納したカード状のメモリ装置17と、前記カード状のメモリ装置17内に格納されたセキュリティデータD2を読み出すためのカードリグ16と、前記D1とD2とを比較する比較手段12Aとからなり、前記比較手段12Aが、前記ハードディスク装置14内に格納されたセキュリティデータD1と前記カード状のメモリ装置17内に格納されたセキュリティデータD2とが同じであることを検出したとき、前記ハードディスク装置14を使用可能な状態にする。



【特許請求の範囲】

【請求項1】 コンピュータ装置の記憶装置であるハードディスク装置のセキュリティシステムであって、

前記ハードディスク装置内に格納したセキュリティデータと、

セキュリティデータを格納したカード状のメモリ装置と、

前記カード状のメモリ装置内に格納されたセキュリティデータを読み出すためのカードリーダと、

前記ハードディスク装置内に格納されたセキュリティデータと前記カードリーダが読み出したカード状のメモリ装置内に格納されたセキュリティデータとを比較する比較手段とからなり、

前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置を使用可能な状態にすることを特徴とするハードディスク装置のセキュリティシステム。

【請求項2】 前記前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置内の所定の領域のみを使用可能な状態にすることを特徴とする請求項1記載のハードディスク装置のセキュリティシステム。

【請求項3】 前記前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じでないことを検出したとき、前記ハードディスク装置の起動を停止するように構成したことを特徴とする請求項1又は2記載のハードディスク装置のセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ハードディスク装置のセキュリティシステムに係わり、特に、ハードディスク装置を駆逐する際、自動的にセキュリティがかかるようにしたハードディスク装置のセキュリティシステムに関する。

【0002】

【従来の技術】 従来のハードディスク装置のセキュリティシステムでは、ハードディスクセキュリティ用のパスワードを、パーソナルコンピュータ本体の不揮発性メモリに保存し、このパスワードを利用してハードディスク装置がセキュリティ（ロック）を解除する。この方法では、ハードディスクを駆逐する場合、一旦セキュリティをかける必要があり、その操作が複雑であるという欠点があった。

【0003】 また、パーソナルコンピュータ本体の不揮

発性メモリ装置上にパスワードが保存されているため、パーソナルコンピュータ本体ごと第三者に渡ったような場合、容易にハードディスクのセキュリティ解除が行われてしまうという問題があった。

【0004】

【発明が解決しようとする課題】 本発明の目的は、上記した従来技術の欠点を改良し、特に、特に、ハードディスク装置を駆逐する際、自動的にセキュリティがかかるようにすると共に、第三者が簡単にセキュリティの解除を行えないようにした新選なハードディスク装置のセキュリティシステムを提供するものである。

【0005】

【課題を解決するための手段】 本発明は上記した目的を達成するため、基本的には、以下に記載されたような技術構成を採用するものである。

【0006】 即ち、本発明に係るハードディスク装置のセキュリティシステムは、第1態様は、コンピュータ装置の記憶装置であるハードディスク装置のセキュリティシステムであって、前記ハードディスク装置内に格納したセキュリティデータと、セキュリティデータを格納したカード状のメモリ装置と、前記カード状のメモリ装置内に格納されたセキュリティデータを読み出すためのカードリーダと、前記ハードディスク装置内に格納されたセキュリティデータと前記カードリーダが読み出したカード状のメモリ装置内に格納されたセキュリティデータとを比較する比較手段とからなり、前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置を使用可能な状態にすることを特徴とするものであり、又、第2態様は、前記前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置内の所定の領域のみを使用可能な状態にすることを特徴とするものであり、又、第3態様は、前記前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとを比較する比較手段とからなり、前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置の起動を停止するように構成したことを特徴とするものである。

【0007】

【発明の実施の形態】 本発明に係るハードディスク装置のセキュリティシステムは、コンピュータ装置の記憶装置であるハードディスク装置のセキュリティシステムであって、前記ハードディスク装置内に格納したセキュリティデータと、セキュリティデータを格納したカード状のメモリ装置と、前記カード状のメモリ装置内に格納されたセキュリティデータを読み出すためのカードリーダと、前記ハードディスク装置内に格納されたセキュリ

ディータと前記カードリッジが読み出したカード状のメモリ装置内に格納されたセキュリティデータとを比較する比較手段とからなり、前記比較手段が、前記ハードディスク装置内に格納されたセキュリティデータと前記カード状のメモリ装置内に格納されたセキュリティデータとが同じであることを検出したとき、前記ハードディスク装置を使用可能な状態にすることを特徴とするものである。

【0008】従って、このハードディスク装置をコンピュータから切り離す際に、特に、ロック状態にするための作業を行うことなく、このハードディスク装置をロック状態にすることができるから、セキュリティを確保にかけることができ、しかも、ロックの解除は、所定のセキュリティデータが書き込まれたカード状のメモリ装置をカードリーダーにセットするだけであるから、ロックの設定、ロック解除が容易であり、セキュリティの性能を著しく向上することを可能にした。

【0009】

【実施例】以下に、本発明に係わるハードディスク装置のセキュリティシステムの具体例を図面を参照しながら詳細に説明する。

【0010】(第1の具体例) 図1、図2は、本発明に係るハードディスク装置のセキュリティシステムの第1の具体例を示す図であって、これらの図には、コンピュータ装置の記憶装置であるハードディスク装置のセキュリティシステムであって、前記ハードディスク装置14内に格納したセキュリティデータD1と、セキュリティデータD2を格納したカード状のメモリ装置(メモリカード)17と、前記カード状のメモリ装置17内に格納されたセキュリティデータD2を読み出すためのカードリーダー16と、前記ハードディスク装置14内に格納されたセキュリティデータD1と前記カードリーダー16が読み出したカード状のメモリ装置17内に格納されたセキュリティデータD2とを比較する比較手段12Aとからなり、前記比較手段12Aが、前記ハードディスク装置14内に格納されたセキュリティデータD1と前記カード状のメモリ装置17内に格納されたセキュリティデータD2とが同じであることを検出したとき、前記ハードディスク装置14を使用可能な状態にすることを特徴とするハードディスク装置のセキュリティシステムが示されている。

【0011】この場合、前記比較手段12Aが、前記ハードディスク装置14内に格納されたセキュリティデータD1と前記カード状のメモリ装置17内に格納されたセキュリティデータD2とが同じであることを検出したとき、前記ハードディスク装置14内の所定の領域のみを使用可能な状態にするように構成しても良い。

【0012】以下に、第1の具体例を更に詳細に説明する。

【0013】図1において、コンピュータ本体11に

は、セキュリティデータD1を格納する記憶領域15が設けられたハードディスク14が接続されている。コンピュータ本体11は、CPU12とBIOS ROM13を有している。BIOS ROM13には、カードリーダー16やハードディスク14の制御プログラムが格納されていて、CPU12は、これらを実行する。カードリーダー16は、コンピュータ本体11に、ポート19を介して接続される。カード状のメモリ装置17には、パスワードなどのセキュリティデータD2を書き込むための記憶領域18が内部に設けられている。次に、本発明のハードディスク装置のセキュリティシステムの動作について、図2のフローチャートを用いて説明する。コンピュータ本体11が起動すると、CPU12は、BIOS ROM13内の制御プログラムにより、ハードディスク装置14の状態を調べる。ハードディスク装置14がロック状態にある場合(ステップS1)、まず、カードリーダー16が、コンピュータ本体11のポート19に接続されていることを確認する(ステップS2)。接続が確認されると、次に、メモリカード17の挿入を要求する(ステップS3)。メモリカード17がカードリーダー16にセットされると、カードリーダー16は、メモリカード17内の記憶領域18に格納されたパスワードD2を読み込む。CPU12は、取得されたパスワードD2とハードディスク装置14上の記憶領域15に設定されているパスワードD1とを比較し(ステップS4)、一致した場合のみ(ステップS5)、ハードディスク14のロック状態を解除し(ステップS6)、起動を実行する(ステップS7)。カードリーダー16が未装着であったり、挿入されたメモリカード17のパスワードD2とハードディスク14のパスワードD1が不一致である場合には、ハードディスク14のロック状態が解除できなかったことを示すメッセージを表示した後(ステップS8)、起動を実行する(ステップS7)。

【0014】(第2の具体例) なお、スマートカード17の複製をN枚作成することで、N人のユーザのアクセスを可能にすることもできる。また、ハードディスク14のロック解除に成功したか否かの情報を基に、コンピュータ本体11のシステムに対するセキュリティをかけるように構成しても良い。

【0015】更に、ハードディスク装置14のロック解除に失敗した場合、アクセスしたユーザは不正な者であると判断し、システムそのものを停止するように構成しても良い。

【0016】

【発明の効果】本発明に係るハードディスク装置のセキュリティシステムは、上述のように構成したので、このハードディスク装置をコンピュータから切り離す際、特に、ロック状態にするための作業を行うことなくロック状態にすることができるから、セキュリティを確保にかけることができ、しかも、ロックの解除は、所定

のセキュリティデータが書き込まれたカード状のメモリ装置をカードリーダーにセットするだけであるから、ロックの設定、ロック解除が容易であり、セキュリティの性能を著しく向上することを可能にした。

【0017】また、従来のように、コンピュータ本体又はハードディスク装置内は、パスワード等を格納した不揮発性のメモリ装置を備えない構成であるから、第三者が、パスワード等のセキュリティデータを解読することが困難であるという優れた特徴を有している。

【図面の簡単な説明】

【図1】本発明に係るハードディスク装置のセキュリティシステムの構成を示すブロック図である。

＊【図2】本発明の動作を説明するフローチャートである。

【符号の説明】

11 コンピュータ本体

12 CPU

13 BIOS ROM

14 ハードディスク装置

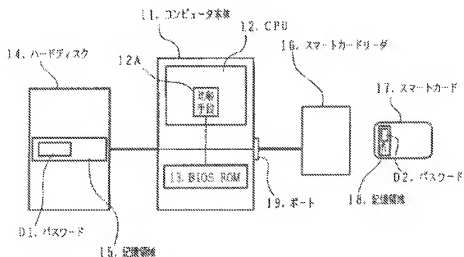
15、18 セキュリティデータの記憶領域

16 カードリーダー

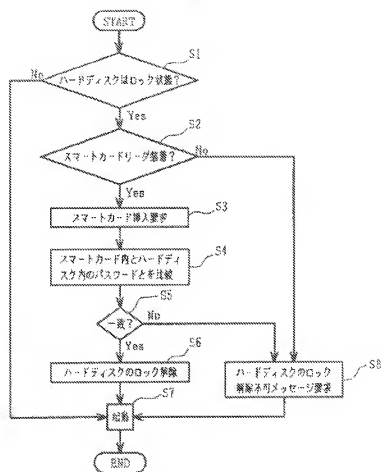
10 15 カード状のメモリ装置（メモリカード）

D1、D2 セキュリティデータ

【図1】



【図2】



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]When it detects that security data which was provided with the following and in which said comparison means was stored in said hard disk drive and security data stored in a storage device of said card shape are the same, A security system of a hard disk drive changing said hard disk drive into an usable state.

Security data which is a security system of a hard disk drive which is the memory storage of computer paraphernalia, and was stored in said hard disk drive.

A storage device of card shape which stored security data.

A card reader for reading security data stored in a storage device of said card shape.

A comparison means to compare security data stored in said hard disk drive with security data stored in a storage device of card shape which said card reader read.

[Claim 2]When it detects that security data in which said said comparison means was stored in said hard disk drive and security data stored in a storage device of said card shape are the same, A security system of the hard disk drive according to claim 1 changing only a predetermined field in said hard disk drive into an usable state.

[Claim 3]When [when security data in which said said comparison means was stored in said hard disk drive and security data stored in a storage device of said card shape are the same] it is and things are detected, A security system of the hard disk drive according to claim 1 or 2 constituting so that starting of said hard disk drive may be suspended.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]When especially this invention conveys a hard disk drive with respect to the security system of a hard disk drive, it relates to the security system of the hard disk drive where it was made for security to start automatically.

[0002]

[Description of the Prior Art]In the security system of the conventional hard disk drive, the password for hard disk security is saved at the nonvolatile memory of a personal computer body, and the security (lock) of a hard disk drive is canceled using this password. In this method, when a hard disk was conveyed, security once needed to be applied and there was a fault that that operation was complicated.

[0003]Since the password was saved on the nonvolatile storage device of a personal computer body, when the whole personal computer body was crossed to a third party, there was a problem that security release of a hard disk will be performed easily.

[0004]

[Problem(s) to be Solved by the Invention]When the purpose of this invention improves the fault of the above-mentioned conventional technology and conveys a hard disk drive especially, make it security start automatically, and. A third party provides the security system of the new hard disk drive prevented from canceling security simply.

[0005]

[Means for Solving the Problem]Fundamentally, this invention adopts technical composition which was indicated below in order to attain the above-mentioned

purpose.

[0006]Namely, the 1st mode of a security system of a hard disk drive concerning this invention, Security data which is a security system of a hard disk drive which is the memory storage of computer paraphernalia, and was stored in said hard disk drive, A card reader for reading security data stored in a storage device of card shape which stored security data, and a storage device of said card shape, It consists of a comparison means to compare security data stored in said hard disk drive with security data stored in a storage device of card shape which said card reader read. When it detects that security data in which said comparison means was stored in said hard disk drive and security data stored in a storage device of said card shape are the same, It is characterized by changing said hard disk drive into an usable state, and ** and the 2nd mode, When it detects that security data in which said said comparison means was stored in said hard disk drive and security data stored in a storage device of said card shape are the same, It is characterized by changing only a predetermined field in said hard disk drive into an usable state, and ** and the 3rd mode, When [whose security data stored in a storage device of said card shape was the same as security data in which said said comparison means was stored in said hard disk drive] it was and things were detected, it constituted so that starting of said hard disk drive might be suspended.

[0007]

[Embodiment of the Invention]The security system of the hard disk drive concerning this invention, The security data which is a security system of the hard disk drive which is the memory storage of computer paraphernalia, and was stored in said hard disk drive, The card reader for reading the security data stored in the storage device of the card shape which stored security data, and the storage device of said card shape, It consists of a comparison means to compare the security data stored in said hard disk drive with the security data stored in the storage device of the card shape which said card reader read, When it detects that the security data in which said comparison means was stored in said hard disk drive and the security data stored in the storage device of said card shape are the same, said hard disk drive is changed into an usable state.

[0008]Therefore, when separating this hard disk drive from a computer, Since this hard disk drive can be changed into a locked position, without doing the work for changing into a locked position especially, Can apply security certainly and, moreover, release of a lock, Since the storage device of card shape with which predetermined security data was written in was only set to the card reader, setting out of a lock and

lock release are easy, and made it possible to improve the performance of security remarkably.

[0009]

[Example]Below, the example of the security system of the hard disk drive concerning this invention is explained in detail, referring to drawings.

[0010](The 1st example) Drawing 1 and drawing 2 are shown figures the 1st example of the security system of the hard disk drive concerning this invention, and to these figures. The security data D1 which is a security system of the hard disk drive which is the memory storage of computer paraphernalia, and was stored in said hard disk drive 14, The storage device (memory card) 17 of the card shape which stored the security data D2, The card reader 16 for reading the security data D2 stored in the storage device 17 of said card shape, It consists of a comparison means 12A to compare the security data D1 stored in said hard disk drive 14 with the security data D2 stored in the storage device 17 of the card shape which said card reader 16 read, When it detects that the security data D1 in which said comparison means 12A was stored in said hard disk drive 14 and the security data D2 stored in the storage device 17 of said card shape are the same, The security system of the hard disk drive changing said hard disk drive 14 into an usable state is shown.

[0011]In this case, when it detects that the security data D1 in which said comparison means 12A was stored in said hard disk drive 14 and the security data D2 stored in the storage device 17 of said card shape are the same, It may constitute so that only the predetermined field in said hard disk drive 14 may be changed into an usable state.

[0012]Below, the 1st example is explained still in detail.

[0013]In drawing 1, the hard disk 14 in which the storage area 15 which stores the security data D1 was formed is connected to the computer body 11. The computer body 11 has CPU12 and BIOS ROM13. The control program of the card reader 16 or the hard disk 14 is stored in BIOS ROM13, and CPU12 controls these in it. The card reader 16 is connected to the computer body 11 via the port 19. The storage area 18 for writing the security data D2 of a password etc. in the storage device 17 of card shape is established in the inside. Next, operation of the security system of the hard disk drive of this invention is explained using the flow chart of drawing 2. If the computer body 11 starts, CPU12 will investigate the state of the hard disk drive 14 with the control program in BIOS ROM13. When the hard disk drive 14 is in a locked position (Step S1), the card reader 16 checks first that the port 19 of the computer body 11 is equipped (Step S2). A check of wearing will require [next] insertion of the memory card 17 (Step S3). If the memory card 17 is set to the card reader 16, the

card reader 16 will read the password D2 stored in the storage area 18 in the memory card 17. CPU12 compares the acquired password D2 with the password D1 set as the storage area 15 on the hard disk drive 14 (step S4). Only when in agreement, the locked position of (Step S5) and the hard disk 14 is canceled (Step S6), and starting is continued (Step S7). When the password D2 of the memory card 17 and the password D1 of the hard disk 14 which had not equipped with the card reader 16 or were inserted are inharmonious. Starting is continued after displaying the message which shows that the locked position of the hard disk 14 was not able to be canceled (Step S8) (Step S7).

[0014](The 2nd example) In addition, N person's user's access can also be enabled by creating N duplicates of the smart card 17. It may constitute so that the security to the system of the computer body 11 may be applied based on the information on whether it succeeded in the lock release of the hard disk 14.

[0015]When the lock release of the hard disk drive 14 goes wrong, the user who accessed may judge that he is an inaccurate person, and he may constitute so that the system itself may be suspended.

[0016]

[Effect of the Invention]The security system of the hard disk drive concerning this invention. Since it constituted as mentioned above, when separating this hard disk drive from a computer. Since it can change into a locked position, without doing the work for changing into a locked position especially, can apply security certainly and, moreover, release of a lock. Since the storage device of card shape with which predetermined security data was written in was only set to the card reader, setting out of a lock and lock release are easy, and made it possible to improve the performance of security remarkably.

[0017]Like before, since the inside of a computer body or a hard disk drive is composition which is not provided with the nonvolatile storage device which stored the password etc., the third party has the outstanding feature that it is difficult to decode the security data of a password etc.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the composition of the security system of the hard disk drive concerning this invention.

[Drawing 2]It is a flow chart explaining operation of this invention.

[Description of Notations]

11 Computer body

12 CPU

13 BIOS ROM

14 Hard disk drive

15 and 18 Security data storage field

16 Card reader

15 A storage device of card shape (memory card)

D1 and D2 Security data

[Translation done.]

Application Showcase

各種パスワードの暗号化と取り出し

Figaro's Password Manager

バージョン: 0.50alpha ライセンス: GPL

<http://www.figaro.org/fpm/>

●ビルドとインストール

FPMは、tarボールとRPMのソース/バイナリパッケージが配布されている。Red Hat系ディストリビューションではRPMパッケージを使うとよいだろう。tarボールからのビルドとインストールも、[/configure] → [make] → [make install] という一般的な手順だ。

●パスワードの保存

[fpm]として起動すると、最初にFPM用のパスワードの入力を求められる。これは、起動時のセキュリティを保つとともに、FPMで管理するユーザー名やパスワードを暗号化する際のキーとしても使われる。

パスワードを入力すると、FPMのウィンドウが開く(図面1)。ウィンドウには、設定済みのエントリのタイトルやURL/コマンド、ユーザー名が一覧表示されている。

エントリを新規作成するには、フー

ルバーの[New]ボタンを押せばいい。ダイアログが開くので、タイトルやユーザー名、パスワードを設定しよう(図面2)。Webベースの掲示板の場合は、[Launcher]を[Web]に設定し、[URL/Arg]にURLを設定しておく。

入力したパスワードは、通常「*」でマスクされて見えないが、[Show Password]ボタンを押すと内容を確認できる。また、[Generate]ボタンで開くダイアログで、パスワードを自動生成することも可能だ。

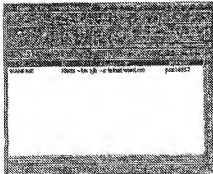
●パスワードの取り出し

情報を取り出したいエントリを選択し、フォーバーの[User]や[Password]ボタンを押すと、クリップボードとプライマリセクションに内容がコピーされ、Ctrl-Vキーやマウスの中ボタンでペーストされる。

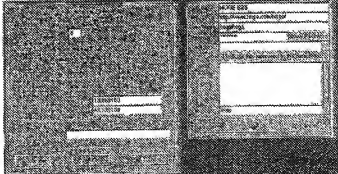
また、[Jump]ボタンを押すと、指定したURLのページをNetscapeで表示する。この場合、ユーザー名はクリップ

ボード、パスワードはプライマリセクションにコピーされ、それぞれAlt-Vキーとマウスの中ボタンでペーストできる。Netscapeのほか、sshや低層のコマンドを起動することも可能で、ユーザー名やパスワードの取り出し方法は柔軟に設定できる(図面3)。

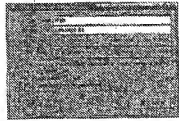
Webブラウザを用いた、ショッピングやオークションなど、ユーザー名とパスワードを要求される機会が増える一方で、FPMを用いれば、モニタの横にパスワードを書きとめたりせずに、スマートな管理が可能になる。



図面1
パスワードを管理しているエントリの一覧が表示される。



図面2
ユーザー名やパスワードなどを設定する。自動生成も可能だ。



図面3
起動するコマンドやユーザー名、パスワードの取り出し方を設定。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-169782

(43)Date of publication of application : 14.06.2002

(51)Int.Cl.

G06F 15/00

G06F 1/00

G06K 17/00

G06K 19/07

H04L 9/32

(21)Application number : 2000-
369216

(71)Applicant : NETTIME CORP

(22)Date of filing :

04.12.2000

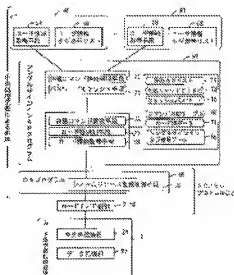
(72)Inventor : MARUYAMA SHINGO

(54) PORTABLE INFORMATION STORAGE MEDIUM, USER USE CONTROL SYSTEM, USER USE CONTROL METHOD AND USER USE CONTROL PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To manage user information in an area managed by a password, to secure high security, to eliminate the need of inputting the password for accessing the managed area whenever a program is used on a user terminal and to improve the convenience of the user terminal.

SOLUTION: Various pieces of user information used in the user terminal are stored in a data storage part 27 being the area where access is managed by the password of a card-type information storage medium 1. At the time of first access to user information, the password is inputted by a user and user information is read from the data storage part 27. At the time of next access to user information, the password is stored and user information is read from the managed data storage part 27 by using the password.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A portable information storage medium which is a portable information storage medium which memorizes User Information used by two or more programs which it is inserted in a user terminal and executed on the user terminal concerned, and is characterized by what is recorded as the User Information concerned can be accessed using a password.

[Claim 2]Are two or more User Information used by two or more programs which it is inserted in a user terminal and executed on the user terminal concerned a portable information storage medium to memorize, and two or more User Information concerned, A portable information storage medium characterized by what is recorded as it can access to each User Information with a common password.

[Claim 3]Are two or more User Information used by two or more programs which it is inserted in a user terminal and executed on the user terminal concerned a portable information storage medium to memorize, and two or more User Information concerned, A portable information storage medium characterized by what is recorded in a field where access is managed with a predetermined password.

[Claim 4]The portable information storage medium according to claim 2 or 3, wherein each User Information is matched with a peculiar identification number and memorized for every User Information.

[Claim 5]It is a user's use control system which manages various kinds of execution and/or processings of a program using User Information which is included in a user terminal and memorized by portable information storage medium, The User Information reading means which reads above-mentioned User Information from a

portable information storage medium of a statement to any 1 paragraph of claim 1 to the claims 4 based on a demand from the above-mentioned program, Have a password inputting means into which a user is made to enter a password based on a read-out demand of the first User Information, and a memory measure which memorizes the above-mentioned password, and the above-mentioned User Information reading means, A user's use control system reading above-mentioned User Information using a password memorized by the memory measure concerned.

[Claim 6]The user's use control system according to claim 5 establishing a demand exclusive control means delivered to said User Information reading means in an order from a demand which made a memory measure memorize a User Information read-out demand from said program, and received it previously.

[Claim 7]The user's use control system according to claim 5 or 6, wherein said User Information reading means performs read-out processing to the portable information storage medium concerned after changing a User Information read-out demand from said program into a demand which can be processed with said portable information storage medium.

[Claim 8]Various kinds of User Information used with a user terminal is stored in a field to which access was managed with a password, Read User Information from a field which made a user enter the above-mentioned password and was managed [above-mentioned] on the occasion of access of the beginning to the User Information concerned, and in the case of access to User Information from next time. A user's use control method reading User Information from a field which memorizes the above-mentioned password and was managed [above-mentioned] using this.

[Claim 9]A user's use control program which reads various kinds of User Information used with a user terminal from a field where it was installed in a user terminal and access was managed with a password, comprising:

A step into which a user is made to enter a password based on a read-out demand of User Information of the beginning from a program currently executed with the above-mentioned user terminal.

A step which reads above-mentioned User Information from a field managed [above-mentioned] using a password memorized by the memory measure concerned based on a read-out demand of User Information from a step which makes a memory measure memorize the above-mentioned password, and a program currently executed with the above-mentioned user terminal.

* NOTICES *

JPO and INPI are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. *** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a portable information storage medium, a user's use control system, the user's use control method, and a user's use control program, and relates to the invention for raising a user's convenience especially.

[0002]

[Description of the Prior Art] Conventionally, each company, government and municipal offices, etc. institute what is called intranet in the company, share information between each company member using the user terminal connected to this, and have been attaining the increase in efficiency of each business, etc.

[0003] Thus, for example in the database etc., when intranet is used, in order to judge whether access may be permitted to the user who has accessed, art, such as user authentication, is generally used. Each user inputs User Information of a password etc. from a user terminal, when such attestation is called for.

[0004] And such a password will be the length which data length becomes long, and an individual cannot memorize certainly, and cannot be inputted, in order to raise the security. Therefore, it is possible to use portable information storage media, such as a smart card used as a banking card, a credit card, a point card, a prepaid card, etc.

[0005] It is each user's making User Information memorize beforehand in this portable information storage medium, and inserting this in the card reading device connected to the user terminal by this, It becomes possible to perform personal authentication, without inputting User Information required in order to access information one by one from an input device.

[0006]However, when predetermined User Information is stored in such a portable information storage medium, a possibility that the User Information concerned will be shortly read from the portable information storage medium cannot be denied thoroughly. And if User Information is acquired from a portable information storage medium, it will become possible to access unjustly.

[0007]Therefore, in the user's use control system to which the personal authentication etc. of the user who uses a user terminal conventionally using such a portable information storage medium are made to perform, access stored User Information in the field managed with the password.

[0008]

[Problem(s) to be Solved by the Invention]By the way, some are remarkable in development of computer technology in recent years and network technology so that it may be represented by the Internet technique currently called what is called World Wide Web etc.

[0009]And open networks, such as such the Internet, by taking in to a part of the infrastructure each company, Rather than the case where an independent network is instituted, a network can be built cheaply and, moreover, management of the absolutely impossible sales department member, etc. can be easily performed now by the former.

[0010]However, when such an open network is used, attestation in two or more steps, such as dial-up information on the Internet, certification information of the firewall to intranet, and certification information in a database, is needed, for example.

[0011]And a portable information storage medium is packed for some of every User Information, or as mentioned above, from the circumstances into which it has developed as a thing for the user authentication in intranet, even if it is good, it is mainly packed for every application, and it is stored in the field managed with the password.

[0012]Therefore, in the case where the database on intranet is accessed from an open network etc., At the time of a dialup connection, at the time of connection with intranet, a password must be entered in many stages at the time of connection with a database, etc. repeatedly, and there are problems — it is hard to use.

[0013]Whenever it starts each application program, a password must be entered, and there are also problems — it is very hard to use.

[0014]Though User Information is managed in the field managed with the password and high security is secured, this invention, Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter

a password. It aims at obtaining the portable information storage medium, the user's use control system, the user's use control method, and user's use control program which pursued the convenience of the user terminal by this.

[0015]

[Means for Solving the Problem]For the above-mentioned purpose, a portable information storage medium of this invention. It is inserted in a user terminal, and it is a portable information storage medium which memorizes User Information used by two or more programs executed on the user terminal concerned, and it is recorded that the User Information concerned can be accessed using a password.

[0016]If this composition is adopted, two or more programs can be used only by holding and reusing a password which a user entered in a user terminal. Therefore, though User Information is managed in a field managed with a password and high security is secured, Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0017]It is a portable information storage medium which memorizes two or more User Information used by two or more programs which a portable information storage medium of this invention is inserted in a user terminal, and are executed on the user terminal concerned, It is recorded that two or more User Information concerned can be accessed to each User Information with a common password.

[0018]If this composition is adopted, two or more User Information used by two or more programs can be read only by holding and reusing a password which a user entered in a user terminal. Therefore, though User Information is managed in a field managed with a password and high security is secured. Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0019]It is a portable information storage medium which memorizes two or more User Information used by two or more programs which a portable information storage medium of this invention is inserted in a user terminal, and are executed on the user terminal concerned, Two or more User Information concerned is recorded in a field where access is managed with a predetermined password.

[0020]If this composition is adopted, two or more User Information used by two or more programs can be read only by holding and reusing a password which a user entered in a user terminal. Therefore, though User Information is managed in a field managed with a password and high security is secured, Whenever it uses a program on

a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0021]Each User Information is matched with a peculiar identification number for every User Information, and a portable information storage medium of this invention is memorized.

[0022]If this composition is adopted, the user can use this about a program installed in common on various kinds of user terminals, without choosing a user terminal. Two or more programs installed in the same user terminal also become possible [using common User Information by them].

[0023]It is a user's use control system which manages various kinds of execution and/or processings of a program using User Information which a user's use control system of this invention is built into a user terminal, and is memorized by portable information storage medium. The User Information reading means which reads above-mentioned User Information from a portable information storage medium of one of the above based on a demand from the above-mentioned program. Having a password inputting means into which a user is made to enter a password based on a read-out demand of the first User Information, and a memory measure which memorizes the above-mentioned password, the above-mentioned User Information reading means reads above-mentioned User Information using a password memorized by the memory measure concerned.

[0024]If this composition is adopted, a memory measure can be made to be able to memorize a password which a user entered based on a demand of a password inputting means, and this can be used common to two or more programs. Therefore, though User Information is managed in a field managed with a password and high security is secured, Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0025]A user's use control system of this invention makes a memory measure memorize a User Information read-out demand from said program, and establishes a demand exclusive control means delivered to said User Information reading means in an order from a demand which received previously.

[0026]If this composition is adopted, even if an acquisition request of User Information occurs simultaneously from two or more programs, the User Information reading means can process this in turn and and certainly. Thereby, without caring about a concurrence of an acquisition request of User Information, the user can use

two or more programs and can provide the high convenience of a user terminal.
[0027]A user's use control system of this invention performs read-out processing to the portable information storage medium concerned, after said User Information reading means changes a User Information read-out demand from said program into a demand which can be processed with said portable information storage medium.

[0028]If this composition is adopted, since the User Information reading means changes a User Information read-out demand from a program into a demand which can be processed with a portable information storage medium, it, A User Information read-out demand in each program, etc. can be programmed without caring about a kind and a standard of a portable information storage medium. Therefore, a program which generates a User Information read-out demand can be developed easily.

[0029]A user's use control method of this invention stores various kinds of User Information used with a user terminal in a field to which access was managed with a password, Read User Information from a field which made a user enter the above-mentioned password and was managed [above-mentioned] on the occasion of access of the beginning to the User Information concerned, and in the case of access to User Information from next time. He memorizes the above-mentioned password and is trying to read User Information from a field managed [above-mentioned] using this.

[0030]If this method is adopted, a password which a user entered is memorized and this can be used also in a program started later. Therefore, though User Information is managed in a field managed with a password and high security is secured, Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0031]A user's use control program of this invention is installed in a user terminal, It is a user's use control program which reads various kinds of User Information used with a user terminal from a field where access was managed with a password, A step into which a user is made to enter a password based on a read-out demand of User Information of the beginning from a program currently executed with the above-mentioned user terminal, Based on a read-out demand of User Information from a step which a memory measure is made to memorize, and a program currently executed with the above-mentioned user terminal, the above-mentioned password, It has a step which reads above-mentioned User Information from a field managed [above-mentioned] using a password memorized by the memory measure concerned.

[0032]If this composition is adopted, a user can be made to be able to enter a

password based on a read-out demand of User Information of the beginning from a program currently executed with a user terminal, and this can be used common to two or more programs. Therefore, though User Information is managed in a field managed with a password and high security is secured, Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password, and thereby, the high convenience of a user terminal can be provided.

[0033]

[Embodiment of the Invention]The portable information storage medium, the user's use control system, the user's use control method, and user's use control program concerning an embodiment of the invention are explained based on figures. The user's use control method is explained as operation of the whole user's use control system. Although each user is provided with various kinds of programs, such as a user's use control program, with the recording medium which recorded the program and in which computer reading is possible, generally, By this embodiment, the above-mentioned program recorded on the recording medium concerned explains as what is already installed in the program store part 15 of a user's use control system.

[0034]Drawing 1 is a system configuration figure showing an example of the user's use control system by the embodiment of the invention 1.

[0035]The user's use control system of this invention The card shape information recording medium 1 as portable information storage media, such as a smart card, This card shape information recording medium 1 is provided with the user terminal 3 provided with the card reading device 2 by which insert and remove are carried out, the net network 4 connected to this user terminal 3, and the databases 5 and 6 which are connected to this net network 4 and hold various kinds of data.

[0036]These databases 5 and 6 memorize the open data of a homepage etc., for example, or memorize data [KUROZUDO / extra sensitive information / in which only some users permit access / operating]. In particular, in being KUROZUDO data, when there is access from the user terminal 3, it performs the user authentication.

[0037]The net network 4 The Internet 7 as an open network, The intranet 9 to which one database 5 was connected while this Internet 7 was accessed via the firewall 8, It has the intranet 11 to which the database 6 and the user terminal 3 of another side were connected while the Internet 7 was accessed via the firewall 10. And if each firewalls 8 and 10 have an access request from the Internet 7, they will generally process user authentication etc., and they are constituted so that it may permit access to the intranet 7, in being eligible personnel.

[0038]The central processing unit (CPU:Central Processing Unit) 12 with which the

user terminal 3 mainly performs various kinds of data processing and control management based on a program. The system memory 13 used in the case of execution of this central processing unit 12 of a program. The timer 14 which performs a timer interrupt to the central processing unit 12 in the time set up by the central processing unit 12, it has the storage device 17 provided with the data storage part (memory measure) 16 which memorizes various kinds of data used in the case of execution of the program store part 15 which memorizes the above-mentioned program, and the program concerned, and the system bath 18 which connects these mutually.

[0039]In this user terminal 3, the peripheral equipment interface part (peripheral equipment I/F part) 19 is further connected to the system bath 18. Various kinds of peripheral devices, such as the input device 20, the display device 21, the print device 22, the communication device 23, and the card reading device 2, are connected to this peripheral equipment interface part 19. This communication device 23 is directly connected to the intranet 11.

[0040]Drawing 2 is a circuit block figure showing an example of the card type information storage medium 1 in the user's use control system of Drawing 1.

[0041]The central processing unit (CPU) 24 with which the card type information storage medium 1 performs various kinds of data processing and control management based on a program. The system memory 25 used in the case of execution of this central processing unit 24 of a program, it has the card memory 28 provided with the data storage part 27 which memorizes various kinds of data used in the case of execution of the program store part 26 which memorizes the above-mentioned program, and the program concerned, and the system bath 29 which connects these mutually. The card I/F part 30 directly connected with the card reading device 2 at the time of card insertion is connected to the above-mentioned central processing unit 24. Although this embodiment explains to the example the smart card of a contact process inserted in the card reading device 2, if it is a portable information storage medium, it will have the same convenience, even if it is a smart card of a noncontact type.

[0042]The data input/output control program 31, the standard command execution program 32, the enciphered program 33, and the program that the other central processing units 24 execute are memorized by the program store part 26. Although the enciphered program 33 may be executed with the central processing unit 24 concerned in this way, in raising a security side further, Independently [the central processing unit 24 concerned], to put side by side separately the cipher-processing

device which performs data processing, and what is necessary is just made to perform encryption and decoding processing here by the unique arithmetic logic which specialized in encryption.

[0043]The data input/output control program 31 is read into the system memory 25 from the central processing unit 12 of the user terminal 3 based on the session setup request transmitted to the card I/F part 30 through the system bus 18, the peripheral equipment I/F part 19, and the card reading device 2, it performs with the central processing unit 24. The central processing unit 24 which executes this data input/output control program 31 receives the command according to standard from the central processing unit 12 of the user terminal 3, and answers the result of execution of the command according to the standard concerned to the central processing unit 12 concerned further. Execution is ended after this response and a session is opened.

[0044]The standard command execution program 32 is read into the system memory 25 according to reception of the above-mentioned command according to standard, and is executed by the central processing unit 24. The central processing unit 24 which executes this standard command execution program 32 performs processing etc. which execute the command according to standard, for example, read predetermined data from the data storage part 27 by that execution.

[0045]When the enciphered program 33 carries out encryption processing or decoding processing, it is read into the system memory 25, and it is executed by the central processing unit 24. By this, make various kinds of User Information encipher, and the data storage part 27 is made to memorize, and it can be decoded and it can be made to use with the user terminal 3 further.

[0046]By the way, as it was only written as the standard command execution program instead of a command execution program, according to the use, many standards exist in the card type information storage medium 1. For example, there are standards, such as a standard enacted since the standard and government and municipal offices which were enacted since the standard and credit company which enacted since a bank provided the service provided service of their company provided the service. The standard original with each is enacted also in the company which provides the security in a company or a net network. Thus, by enacting a standard original with each, each company can provide the management service of User Information with higher safety.

[0047]Therefore, in various kinds of application AP programs using these services, a different command (command according to standard) for every standard must usually be transmitted to the card type information storage medium 1, and, thereby,

predetermined User Information must be acquired.

[0048]In the data storage part 27, with the card identity number 34 etc. In the network login information 35, the database login information 36, the client login information 37, the electronic money information 38, the user identification information 39, the user terminal login information 40, the dial-up information 41, the other above-mentioned user terminals 3, etc. Various kinds of User Information to be used is memorized.

[0049]This card identity number 34 is a peculiar number according to the card vendor which provides the card shape information recording medium 1 concerned, the kind of card within the vendor concerned, etc. Thereby, the kind and the corresponding standard of the card shape information recording medium 1 concerned can be judged.

[0050]Drawing 3 is an explanatory view showing an example of the data mapping of the data storage part 27 in the card type information storage medium 1 of drawing 2.

[0051]The data storage part 27 consists of the management domain 42 of one master file set up from the head position, and the management domain 43 of two or more DEDIKETO files. Each management domains 42 and 43 are set up as a field which continued on the data storage part 27, respectively.

[0052]In the management domain 42 of a master file, the master file 44 (portion bundled with □ which starts in "MF tag number" in the management domain 42 in drawing 3) is stored in the head position. One or more elementary files 45 (portion bundled with □ which starts in "EF tag number" in the management domain 42 in drawing 3) are stored after it.

[0053]In the management domain 43 of each DEDIKETO file. The DEDIKETO file 46 (portion bundled with □ which starts in "DF tag number" in the management domain 43 in drawing 3) is stored in the head position. One or more elementary files 47 (portion bundled with □ which starts in "EF tag number" in the management domain 43 in drawing 3) are stored after it. And each above-mentioned User Information is stored in the data field of the elementary file 47 stored in the management domain 43 of this DEDIKETO file so that it may mention later.

[0054]The data mapping method of the data storage part 27 is explained using drawing 4.

[0055]According to this embodiment, as shown in drawing 4 (A), the data storage part 27 is classified and managed in the management domain 42 of one master file, and the management domain 43 of two or more DEDIKETO files.

[0056]The management domain 42 of a master file is set up as a field including the head position of the data storage part 27, and it is defined as the management domain 43 of each DEDIKETO file becoming one address space which follows each in the

other field for every predetermined data size, and for example, when it is going to realize single sign-in (enable use of all the programs for example, in the user terminal 3 by one ID) in two or more user terminals 3 of all, Only the number of the user terminals 3 which carry out the insert and remove of the card type information storage medium 1 concerned should form the management domain 43 of each DEDIKETO file. In drawing 4, single sign-in is realizable in the eight user terminals 3. [0057]The master file (in drawing 4 (A), it is written as [MF].) 44 is stored in the head position, and various kinds of elementary files ([EF] and notation) 45 are stored in the management domain 42 of a master file following it. The DEDIKETO file ([DF] and the notation) 46 is stored in the head position, and various kinds of elementary files ([EF] and notation) 47 are stored in the management domain 43 of each DEDIKETO file following it.

[0058]The master file [MF] 44 consists of a tag field, a size field, and a data field, as shown in drawing 4 (B). The specific tag number beforehand defined based on the standard of the card type information storage medium 1 concerned, etc. is assigned to the tag field of the master file [MF] 44. The name (tag-field value) of all the DEDIKETO files [DF] 46 etc. which were provided in the card type information storage medium 1 concerned are stored in the data field of the master file [MF] 44, for example. The value according to size, such as a number of bytes of this data field and the number of bits, is stored in the size field.

[0059]The DEDIKETO file [DF] 46 consists of a tag field, a size field, and a data field, as shown in drawing 4 (C). The tag number of a mutually different value peculiar to each is assigned to the tag field of the DEDIKETO file [DF] 46. Let this value be a different value also from the tag number of the tag field of the above-mentioned master file 44. The password required in order to access to the elementary file [EF] 47 in the management domain 43 of the DEDIKETO file concerned etc. are stored in the data field of the DEDIKETO file [DF] 46, for example.

[0060]Elementary file [EF] 45 and 47 consist of a tag field, a size field, and a data field, as shown in drawing 4 (D). Elementary file [EF] The tag number of a mutually different value peculiar to each is assigned to the tag field of 45 and 47. Let this value be a peculiar value for every User Information while making it into a different value also from the value of the tag number of the above-mentioned master file 44, and the value of the tag number of the above-mentioned DEDIKETO file 46. In using two or more User Information in one program, it considers it as a peculiar value for every User Information.

[0061]an elementary file [EF] — to the data field of 45 and 47. When it is stored in the

management domain 43 of a DEDIKETO file, User Information itself — or the data for managing the whole card, such as a card identity number, when what was enciphered is stored and it is stored in the management domain 42 of a master file — as it is — or it is enciphered and stored.

[0062] Thus, in the card type information storage medium 1 of this embodiment, a peculiar tag number is matched to each and each User Information and a card identity number are managed as a separate file (elementary file [EF] 47). Each file (elementary file [EF] 47), every two or more application AP program 49, 50, and 51 (refer to drawing 5) which you want to execute by 1 time of password input, or user terminal 3 — and it will be classified into the field (management domain 43 of a DEDIKETO file) to which the access control was carried out according to one password.

[0063] In order to read predetermined User Information from the card type information storage medium 1 with which such data mapping is made, The management domain 43 of the DEDIKETO file which stores the User Information concerned is made to pinpoint in the central processing unit 24 first fundamentally. Next, after it made the password stored in the DEDIKETO file [DF] 46 concerned compare and the password is in agreement, The elementary file [EF] 47 which stores above-mentioned User Information is made to choose, and above-mentioned User Information is made further read from the data field of the elementary file 47.

[0064] Drawing 5 is an explanatory view showing the example of composition of the program store part 15 in the user's use control system of drawing 1.

[0065] In the program store part 15 of this storage device 17, as the program installed from the recording medium besides a graphic display — the operating system program (OS program) 48 — further, . Perform with the central processing unit 12 under management of this OS program 48. A communication application application program. (Communication application AP program) 49, the client application application program (client application AP program) 50, the electronic commerce application application program (electronic commerce application AP program) 51, a single sign-in application program. (Single sign-in AP program) 52 and the application program which the other central processing units 12 execute are memorized.

[0066] The OS program 48 consists of a program for executing various kinds of application programs on the system resource supervisory control program 53, the program exclusive control program 54, the communications program 55 between programs, and other user terminals.

[0067] The system resource supervisory control program 53 is first read into the system memory 13 according to powering on to the user terminal 3, etc., and is

executed by the central processing unit 12. The central processing unit 12 (equivalent to the system resource supervisor control means 56 in drawing 5) which executes the system resource supervisory control program 53, Interruption from those, such as the timer 14 and the peripheral equipment devices 20, 21, 22, 23, and 2, is managed, or data and a command are mainly outputted and inputted between the timer 14 and the peripheral equipment devices 20, 21, 22, 23, and 2.

[0066]Especially the central processing unit 12 that executes the system resource supervisory control program 53, In accessing the card type information storage medium 1, the session was established between the card type information storage media 1 each time, the command was transmitted to the card type information storage medium 1 on it, and it has received the response data from the card type information storage medium 1. The central processing unit 12 with which after the response reception concerned executes the system resource supervisory control program 53 opens the above-mentioned session. Thus, it enables two or more application programs (AP program) to access individually and directly the degree of access to the card type information storage medium 1 to the one card type information storage medium 1 by establishing and opening a session.

[0069]The command transmission procedure over such a card type information storage medium 1 is being unified in data-communications standards (protocol), such as ISO7816-3, now.

[0070]The program exclusive control program 54 is first read into the system memory 13 according to powering on to the user terminal 3, etc., and is executed by the central processing unit 12. The central processing unit 12 which executes the program exclusive control program 54, While reading a predetermined program into the system memory 13 according to the above-mentioned interruption etc., mainly, The performance schedule between two or more programs read on the system memory 13 is managed by time-sharing etc., and the central processing unit 12 is made to execute each program.

[0071]Scheduling of these system resource supervisory control program 53 and the program exclusive control program 54 is carried out so that it may perform periodically with the central processing unit 12.

[0072]The communications program 55 between programs is a program which controls the data between two or more programs, and delivery of a command, and when data and a command are outputted from a certain program, it is executed with the central processing unit 12.

[0073]Communication application AP program 49 is provided with the User

Information acquisition program 57 and the User Information tag number list 58, is read into the system memory 13 according to the interruption request from the input device 20, etc., and is executed by the central processing unit 12. The central processing unit 12 which executes this communication application AP program 49 establishes the virtual connection of a predetermined zone on the net network 4 using the communication device 21.

[0074]The User Information tag number list 58 is a list which matched User Information and the tag number (henceforth the [EF] tag number) of an elementary file [EF] about all the User Information used by communication application AP program 49.

[0075]In the time of the login attestation to the net network 4 or the databases 5 and 6, etc., the User Information acquisition program 57 is suitably read into the system memory 13 with execution of communication application AP program 49, and is executed by the central processing unit 12. The central processing unit 12 (equivalent to the User Information acquisition means 59 in drawing 6) which executes the User Information acquisition program 57, The [EF] tag number corresponding to User Information which is needed by communication application AP program 49 is acquired from the User Information tag number list 58, Processing which delivers the common-lead access command which specified this [EF] tag number to single sign-in AP program 52 by communication between programs is performed.

[0076]Client application AP program 50, It is a program for performing various kinds of data processing using the data on the database 5 and 6, etc., and is read into the system memory 13 according to the interruption request from the input device 20, etc., and the central processing unit 12 performs. Electronic commerce application AP program 51 is a program for receiving various kinds of goods and service by which offer sale is carried out with the net network 4 using electronic money (electronic token), It is read into the system memory 13 according to the interruption request from the input device 20, etc., and the central processing unit 12 performs. And the User Information acquisition program 57 which acquires various kinds of User Information from the card type information storage medium 1 also in these application AP programs 50 and 51, It had the User Information tag number list 58 which memorized the [EF] tag number used in order that this User Information acquisition program 57 may acquire each User Information. and using these, from the card type information storage medium 1, it was begun suitably to read predetermined User Information, and it is used.

[0077]The [EF] tag number of each User Information registered into each User Information tag number list 58 is a number which is mutually different for every User

Information, as mentioned above, and it is a number set up in common in two or more users for every kind of this User Information. It does not matter at all whether it uses the same User Information in two or more application AP programs or uses over multiple times in the same application AP program.

[0078]It is read into the system memory 13 because single sign-in AP program 52 receives the acquisition requests (common-leads access command etc. which specified the above-mentioned [EF] tag number) of User Information from various kinds of above-mentioned application AP programs 49, 50, and 51. The central processing unit 12 performs. This single sign-in AP program 52, By the password input of 1 time by a user, if possible, in order to close, use of two or more above-mentioned application AP programs 49, 50, and 51. The common command exclusive control program 60, the common command conversion program 61, the bus word cache program 62, the card insert-and-remove monitoring program 63, the card kind discrimination program 64, the card identity number tag number data 65, the single sign-in tag number data 66, It has the card identity list of number 67 classified by standard, the command correspondence table 68, etc.

[0079]In order to judge the kind of card type information storage medium 1, and the standard of the command according to standard which can be executed with the card type information storage medium 1, the card identity list of number 67 classified by standard. It is the list which matched the kind concerned and the standard concerned to each card identity number provided from each card vendor. It can be judged from which vendor the card type information storage medium 1 inserted in the card reading device 2 is supplied by this based on a card identity number.

[0080]The card identity number tag number data 65 is data of the [EF] tag number matched with the above-mentioned card identity number. Let this card identity number tag number be the only predetermined number irrespective of a card vendor, the above-mentioned kind, a standard, etc. in the service concerned.

[0081]a single --- sign-in --- a tag number --- data --- 66 --- plurality --- application --- an AP program --- 49 --- 50 --- 51 --- a unit --- or --- a user terminal --- three --- a unit --- attestation --- carrying out --- a sake --- these --- service --- providing --- a vendor --- a company --- specifying --- [--- EF ---] --- a tag number --- data --- it is .

[0082]The command correspondence table 68 is a table which matched the command according to standard in each standard to each common command. Thereby, if the standard of the card type information storage medium 1 can be specified, the command according to standard which should transmit to the card type information storage medium 1 concerned based on a common command can be specified.

[0083]The card insert-and-remove monitoring program 63 is read into the system memory 13 at the time of starting of single sign-in AP program 52, and is periodically executed with the central processing unit 12 as a thread after that, corresponding to a timer interrupt. The central processing unit 12 (equivalent to the card insert-and-remove monitor means 69 in [drawing 6](#)) which executes the card insert-and-remove monitoring program 63, For example, if the card insertion detection flag in the card reading device 2, etc. are supervised periodically and insertion of the card type information storage medium 1 is detected first, the starting information to the card kind decision program 64 will be outputted.

[0084]When the card type information storage medium 1 is extracted, While notifying the notice of a stop (call-back) to all the application AP programs registered into all the programs 60, 61, 62, 63, and 64 and the execution AP list 75 mentioned later which constitute single sign-in AP program 52, All the data which the system memory 13 and the data storage part 16 were made to memorize in single sign-in AP program 52 is eliminated.

[0085]Like [at the time of thereby for example making two or more User Information acquisition programs 57, ..., 57 supervise the insert and remove of the card type information storage medium 1 individually], Without wasting a system memory vainly multiply, the card type information storage medium 1 can extract, and execution of two or more application AP programs can be stopped according to operation.

[0086]The card kind discrimination program 64 is read into the system memory 13 according to the starting information from the card insert-and-remove monitoring program 63, and is executed with the central processing unit 12. The central processing unit 12 (equivalent to the card kind judging means 70 in [drawing 6](#)) which executes the card kind discrimination program 64, The card identity number tag number data 65 is specified, reading access is carried out at the card type information storage medium 1, the card identity number acquired according to this is compared with the card identity list of number 67 classified by standard, and the kind and standard of the card type information storage medium 1 inserted in the card reading device 2 are judged. The data storage part 16 is made to memorize by using the decision result as the card seed data 71 (refer to [drawing 6](#)).

[0087]The common command conversion program 61 is read into the system memory 13 from the User Information acquisition program 57 based on a common command being outputted, and is executed with the central processing unit 12. the central processing unit 12 (setting to [drawing 6](#) — **** — equivalent to the common command conversion method 72 as a User Information reading means) which

executes the common command conversion program 61. The standard which should change a common command using the card seed data 71 is judged, and the predetermined command according to standard is generated from the command correspondence table 68 using this standard and common command (extraction). The command according to standard extracted from the command correspondence table 68 as a result of this processing may consist of two or more commands according to standard which aligned in predetermined order, if there is also a thing.

[0088]The central processing unit 12 which executes the common command conversion program 61. The command according to standard which extracted [above-mentioned] is transmitted to the system resource supervisory control program 53 by communication between programs, and it is made to transmit to the central processing unit 24 of the card type information storage medium 1 from this system resource supervisory control program 53.

[0089]The central processing unit 12 which executes the common command conversion program 61 notifies to each User Information received from the system resource supervisory control program 53 to predetermined application AP programs 49, 50, and 51.

[0090]The common command exclusive control program 60 is read into the system memory 13 with the common command conversion program 61, and is executed with the central processing unit 12. The central processing unit 12 (equivalent to the common command exclusive control means 73 as a demand exclusive control means in drawing 9) which executes the common command exclusive control program 60. Set the common command from two or more User Information acquisition programs 57, ..., 57 to common command FIFO74, and the data storage part 16 is made to memorize. It performs from the common command inputted previously. and if execution of the common command concerned is completed, the following common command will be performed exclusively one by one.

[0091]The data storage part 16 is made to memorize the central processing unit 12 which executes this common command exclusive control program 60 by considering the list of all the application AP programs 49, 50, and 51 which receive a common command and have not been ended as the execution AP list 75.

[0092]The bus word cache program 62 in the case of execution of the beginning of these common command conversion program 61 or the common command exclusive control program 60. It is read into the system memory 13 based on the cash password 76 (refer to drawing 9) not being stored in the data storage part 16 etc., and performs with the central processing unit 12. The central processing unit 12 (equivalent to the

password cache means 77 as a password inputting means in drawing 6 which executes the bus word cache program 62. The window etc. which make the password for single sign-in enter into the display device 21 are displayed, the character string etc. which were inputted to this are acquired, and it stores in the data storage part 16 by making this into the cash password 76.

[0093]Here, the meaning of command interpreter processing of the above-mentioned common command by the common command conversion program 61 using the command correspondence table 68 is explained in detail.

[0094]In order to secure security etc., he is trying for the vendor of each card type information storage medium 1 to make the reading and writing of data to the data storage part 27 control by a command system original with each, as mentioned above. He dares to build an original command system and is trying for this to secure high security and attestation in the vendor related to security or attestation especially. Therefore, in the former, when the User Information acquisition program 57 was developed, the program which acquires User Information in each procedure independently about all the standards used in the application AP program in which the program is included had to be created. That is, when it was going to make one application AP program run on the card type information storage medium 1 based on two or more standards, only the number of the standards had to develop the program for acquiring User Information.

[0095]In order to avoid this problem, the command correspondence table 68 is formed in this embodiment. In each application AP program, the common command was made to output from the User Information acquisition program 57, and the common command of a common command conversion program 61 smell lever is changed into the command according to standard.

[0096]In each application AP program by this, Since it can respond to two or more standards only by developing one program described with the common command, the necessity that he is completely conscious of the standard of two or more card type information storage media 1 which each is going to use is lost, and development becomes very easy.

[0097]In this embodiment, the make lump of command correspondence table 68 the very thing is also elaborated further.

[0098]When a special measure is not taken, a common command is defined in this way. When it is going to carry out command interpreter processing for this using the command correspondence table 68, for every common command, the command according to standard of the number of all the standards will have to be made to

correspond to the command correspondence table 68 independently, and the command list of huge data size will be needed for it.

[0099]However, the card type information storage medium 1 so that it may be represented by the above-mentioned smart card, it is mainly used for personal authentication or security, and in order to access the management domain 43 of a DEDIKETO file mentioned above, for example, the unnecessary command according to standard is essentially adopted as the command according to standard provided by each vendor for such the purpose in many cases. There are many these things used only by making the unnecessary command according to standard essentially the fundamental command according to standard and set.

[0100]That is, to the command according to standard in the card type information storage medium 1, In order to access to data, the special command according to standard (command according to standard which cannot be used only in a specific standard) original with each standard other than the fundamental command according to standard (in two or more standards, it is a command according to standard available in common) which is originally needed for a target exists.

[0101]In this embodiment, an example is taken by the peculiarity of the command according to standard in such a card type information storage medium 1, Make only the command according to standard fundamental to the basic command list to which each common command is made to correspond directly correspond it, and about the special command according to standard original with the above-mentioned standard. It is considered as the command correspondence table 68 which added the addition command set to the basic command list concerned suitably based on type-of-card data. Type-of-card data is used for judgment of whether the command according to standard which added the special command according to standard original with a standard is generated, and no.

[0102]The small total data volume can describe the command correspondence table 68 rather than the command correspondence table at the time of providing the command list which includes the special command according to standard by this, and the command list which does not contain it for every command according to standard. As a result, facilitating of development of the User Information acquisition program 57 and reduction of the data volume of the command correspondence table 68 can be reconciled.

[0103]Next, operation of such a user's use control system is explained.

[0104]If the power supply of the user terminal 3 is switched on, after checking that the system memory 13 etc. are normal, the central processing unit 12 will read into

the system memory 13 the OS program 48 memorized by the program store part 15, and will perform this. Thereby, various kinds of peripheral devices 20, 21, 22, 23, and 2 will be in the state where it was managed by the central processing unit 12.

[0105]The system resource supervisory control program 53 of this OS program 48 and the program exclusive control program 54 are periodically executed for every interruption from the timer 14, or predetermined time after the above-mentioned initial setting. By this, the central processing unit 12 managing the interruption request from the peripheral devices 20, 21, 22, 23, and 2, the data input/output to the peripheral devices 20, 21, 22, 23, and 2, etc. Various kinds of application programs can be executed in time-sharing.

[0106]After initial setting of the user terminal 3 by such an OS program 48 is made, according to the operation to a user's input device 20, etc. for example, If the starting request to communication application AP program 49 is inputted into the central processing unit 12 at the beginning, the central processing unit 12 will read application AP program 49 concerned into the system memory 13 from the program store part 15, and will perform this.

[0107]And in this communication application AP program 49, in order to acquire network login information and database login information from the card type information storage medium 1, the User Information acquisition program 57 is started.

[0108]The central processing unit 12 which executes this User Information acquisition program 57, Search the User Information tag number list 58, and the [EF] tag number corresponding to the above-mentioned network login information or database login information is acquired, The common user information read-out command for reading User Information corresponding to this [EF] tag number is delivered to the common command exclusive control program 60 by the notice between programs.

[0109]The central processing unit 12 which executes the common command exclusive control program 60 delivers the above-mentioned common user information read-out command to the common command conversion program 61 while registering communication application AP program 49 concerned into the execution AP list 75.

[0110]The character string which the password cache program 62 was executed with the central processing unit 12, and the user inputted as a result using the input device 20 etc. is memorized by the data storage part 16 as the cash password 76. Make it more desirable to encipher and memorize the above-mentioned character string in this data storage part 16.

[0111]The central processing unit 12 which executes the common command conversion program 61. The command according to standard for ordering the

above-mentioned common user information read-out command processing equivalent to it, to the central processing unit 24 of the card type information storage medium 1 using the card seed data 71 and the command correspondence table 68 is generated, and this is delivered to the system resource supervisory control program 53.

[0112]The area selection command as which the command according to standard generated here, for example, makes the central processing unit 24 choose the management domain 43 of the DEDIKETO file which used the single sign-in tag number data 66, The command according to collation standard for making the password and the cash password 76 of the DEDIKETO file 46 of the management domain 43 concerned compare in the central processing unit 24. The command according to file selection standard as which the central processing unit 24 is made to choose the elementary file 47 which stores the above-mentioned [EF] tag number. It consists of a command according to read-out standard to which data is made to read from the data field of the selected elementary file 47, and a command according to transmitting standard for making the read data concerned transmit.

[0113]The central processing unit 12 which executes the system resource supervisory control program 53. Through the course from the system bath 18 to the card I/F part 30, based on a PC/SC protocol etc., a session is established between the central processing units 24 of the card type information storage medium 1 which executes the data input/output control program 31, and each command according to standard is transmitted. The central processing unit 24 of the card type information storage medium 1 will execute the standard command execution program 32, if each command according to standard is received.

[0114]The central processing unit 24 of the card type information storage medium 1 receives the command according to standard of all above, and carries out sequential execution in the order of reception. With the card type information storage medium 1, it is performed by processing of the suitable command according to standard which suited each standard by this. and the central processing unit 12 of the user terminal 3, irrespective of the kind of card type information storage medium 1, the network login information and database login information which were matched with the [EF] tag number are acquirable from the card type information storage medium 1.

[0115]User Information acquired from these card type information storage media 1. From the central processing unit 12 which operates based on the common command conversion program 61. The central processing unit 12 which wins popularity to the User Information acquisition program 57 of communication application AP program 49, is passed to it, and executes communication application AP program 49. It becomes

possible by establishing the virtual connection to the intranets 9 and 11 by transmitting network login information from the communication device 21, or transmitting database login information from the communication device 21 to write the data on the database 5 and 6.

[0116] Thus, after communication application AP program 49 accesses the card type information storage medium 1. When client application AP program 50 acquires client login information using the User Information acquisition program 57. Since the password for single sign-in is stored in the data storage part 16 as the cash password 76, the password cache program 62 is not started.

[0117] Similarly, when electronic commerce application AP program 51 acquires electronic money information using the User Information acquisition program 57. Since the password for single sign-in is stored in the data storage part 16 as the cash password 76, the password cache program 62 is not started.

[0118] The central processing unit 12 with which it will execute the common command exclusive control program 60 working if the common command conversion program 61 receives a new common command, Common command FIFO 74 is made to memorize this common command one by one, and if execution of the common command inputted previously is completed, processing which delivers the following common command to the common command conversion program 61 one by one will be performed.

[0119] Thus, User Information used by two or more application AP programs 49, 50, and 51 is stored in the management domain 43 of the DEDIKETO file managed with one password. If a password is entered once, the user can use application AP programs 49, 50, and 51 of these plurality by carrying out cash to the data storage part 16, until the use ends the password which the user entered. Thereby, single sign-in service can be provided to a user.

[0120] If access to the card type information storage medium 1 by two or more above application AP programs 49, 50, and 51 is summarized, it will become a concept as shown in drawing 6. The User Information read-out demand from each application AP program is transmitted to a lower means in order from the means of the figure upper part, and the response of User Information over it is transmitted to an upper means in order from the means of the figure bottom.

[0121] Although an above embodiment is a suitable embodiment of this invention, in the range which does not deviate from the gist of this invention, various change is possible for it. For example, although the above-mentioned embodiment described the case of what a user uses directly as the user terminal 3. For example, in addition, a credit card, a prepaid card, an automatic-accounts-transfer card, It is provided in the

user terminal which the salesclerk who processes the payment by electronic money etc. uses, the entrance to a building, etc., and can use suitably also in the user terminal for managing receipts and payments of the user to the building concerned, etc.

[0122]Although only the number of the user terminals 3 which carry out the insert and remove of the storage 1 concerned forms the management domain 43 of a DEDIKETO file provided in the card type information storage medium 1 concerned and it can be made to perform single sign-in in all the user terminals 3 in this embodiment, For example, about User Information used in the application AP program accessed to the high data of confidentiality, etc. Even if there is the other application AP program used on the same user terminal 3, it manages to the management domain 43 of a different DEDIKETO file from it, and it does not matter even if it makes it make a password enter separately. In this case, the number of the management domains 43 of a DEDIKETO file provided in the card type information storage medium 1 increases more than the number of the user terminals 3 which carry out the insert and remove of it. On the contrary, it may not set up use the management domain 43 of one DEDIKETO file in two or more user terminals 3 also until it says.

[0123]In this embodiment, the user's use control program 57 is started at the time of starting of first application AP program 49, Although he is trying to make the password for accessing to the management domain 43 of the DEDIKETO file used with the user terminal 3 concerned in this timing enter, it may be made to make the password concerned enter at the time of starting of the OS program 48. In this case, it becomes the single sign-in service for every user terminal 3 instead of the single sign-in service to two or more application AP programs 49, 50, and 51.

[0124]Although this embodiment explained the card type information storage medium 1 as an example as a portable information storage medium, Even if it is a portable telephone terminal incorporating the SPOM (self-programable one-chip microcomputer) type IC chip etc. which are standardized in ISO7816, Other small removable memory devices etc. can be used similarly.

[0125]

[Effect of the Invention:]As mentioned above, though User Information is managed in this invention in the field managed with the password and high security is secured. Whenever it uses a program on a user terminal, in order to access the managed field concerned, it is not necessary to enter a password. The portable information storage medium, the user's use control system, the user's use control method, and user's use control program which pursued the convenience of the user terminal by this can be

obtained.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a system configuration figure showing an example of the user's use control system by the embodiment of the invention 1.

[Drawing 2]It is a circuit block figure showing an example of a card type information storage medium in the user's use control system of drawing 1.

[Drawing 3]It is an explanatory view showing an example of the data mapping of a data storage part in the card type information storage medium of drawing 2.

[Drawing 4]It is an explanatory view of the data mapping method in the data storage part shown in drawing 3.

[Drawing 5]It is an explanatory view showing the example of composition of a program store part in the user's use control system of drawing 1.

[Drawing 6]In the user's use control system of drawing 1, it is a key map showing access to the card type information storage medium by two or more application AP programs.

[Description of Notations]

- 1 Card shape information recording medium (portable information storage medium)
- 2 Card reading device
- 3 User terminal
- 4 Net network
- 5 and 6 Database
- 7 Internet
- 8 and 10 Firewall
- 9 and 11 Intranet

- 12 Central processing unit (CPU)
- 13 System memory
- 14 Timer
- 15 Program store part
- 16 Data storage part (memory measure)
- 17 Storage device
- 18 System bath
- 19 Peripheral equipment interface part (peripheral equipment I/F part)
- 20 Input device
- 21 Display device
- 22 Print device
- 23 Communication device
- 24 Central processing unit (CPU)
- 25 System memory
- 26 Program store part
- 27 Data storage part
- 28 Card memory
- 29 System bath
- 30 Card I/F part
- 31 Data input/output control program
- 32 Standard command execution program
- 33 Enciphered program
- 34 Card identity number
- 35 Network login information
- 36 Database login information
- 37 Client login information
- 38 Electronic money information
- 39 User identification information
- 40 User terminal login information
- 41 Dial-up information
- 42 The management domain of a master file
- 43 The management domain of a DEDIKETO file
- 44 Master file
- 45 and 47 Elementary file
- 46 DEDIKETO file
- 48 Operating system program (OS program)

49 Communication application application program (communication application AP program)

50 Client application application program (client application AP program)

51 Electronic commerce application application program (electronic commerce application AP program)

52 Single sign-in application program (single sign-in AP program)

53 System resource supervisory control program

54 Program exclusive control program

55 A communications program between programs

56 System resource supervisor control means

57 User Information acquisition program

58 User Information tag number list

60 Common command exclusive control program

61 Common command conversion program

62 Bus word cache program

63 Card insert-and-remove monitoring program

64 Card kind discrimination program

65 Card identity number tag number data

66 Single sign-in tag number data

67 The card identity list of number classified by standard

68 Command correspondence table

69 Card insert-and-remove monitor means

70 Card kind discriminating means

71 Card seed data

72 Common command conversion method (User Information reading means)

73 Common command exclusive control means (demand exclusive control means)

74 Common command FIFO

75 Execution AP list

76 Cash password

77 Bus word cache means (password inputting means)

[Translation done.]

【特許請求の範囲】

【請求項1】 ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用するユーザ情報を記憶する携帯情報記憶媒体であって、

当該ユーザ情報は、パスワードを用いてアクセスできるように記録されていることを特徴とする携帯情報記憶媒体。

【請求項2】 ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用する複数のユーザ情報を記憶する携帯情報記憶媒体であって、

当該複数のユーザ情報は、共通のパスワードにてそれぞれのユーザ情報に対してアクセスできるように記録されていることを特徴とする携帯情報記憶媒体。

【請求項3】 ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用する複数のユーザ情報を記憶する携帯情報記憶媒体であって、

当該複数のユーザ情報は、所定のパスワードによりアクセスが管理されている領域内に記録されていることを特徴とする携帯情報記憶媒体。

【請求項4】 各ユーザ情報は、ユーザ情報毎に固有の識別番号に対応付けられて記憶されていることを特徴とする請求項2または請求項3記載の携帯情報記憶媒体。

【請求項5】 ユーザ端末に組み込まれ、携帯情報記憶媒体に記憶されているユーザ情報を利用して各種のプログラムの実行およびまたは処理を管理するユーザ使用制御システムであって、

上記プログラムからの要求に基づいて、請求項1から請求項4の内のいずれか1項に記載の携帯情報記憶媒体から上記ユーザ情報を読み出すユーザ情報読出手段と、最初のユーザ情報の読出手段に基づいてユーザにパスワードを入力させるパスワード入力手段と、

上記パスワードを記憶する記憶手段と、を備え、

上記ユーザ情報読出手段は、当該記憶手段に記憶されているパスワードを用いて上記ユーザ情報を読み出すことを特徴とするユーザ使用制御システム。

【請求項6】 前記プログラムからのユーザ情報読出手段を記憶手段に記憶させ、先に受け付けた要求から順番に前記ユーザ情報読出手段に受け渡す要求排他制御手段を設けたことを特徴とする請求項5記載のユーザ使用制御システム。

【請求項7】 前記ユーザ情報読出手段は、前記プログラムからのユーザ情報読出手段を、前記携帯情報記憶媒体で処理可能な態様に変換した上で当該携帯情報記憶媒体に対する読出し処理を行うことを特徴とする請求項5または請求項6記載のユーザ使用制御システム。

【請求項8】 ユーザ端末で利用する各種のユーザ情報をパスワードにてアクセスが管理された領域に格納し、当該ユーザ情報への最初のアクセスの際にユーザに上記パスワードを入力させて上記管理された領域からユーザ情報を読出し、

次回からのユーザ情報へのアクセスの際には、上記パスワードを記憶しておき、これを利用して上記管理された領域からユーザ情報を読出すことを特徴とするユーザ使用制御方法。

【請求項9】 ユーザ端末にインストールされ、パスワードにてアクセスが管理された領域からユーザ端末で利用する各種のユーザ情報を読み出すユーザ使用制御プログラムであって、

上記ユーザ端末にて実行されているプログラムからの最初のユーザ情報の読出手段に基づいてユーザにパスワードを入力させるステップと、

上記パスワードを記憶手段に記憶させるステップと、上記ユーザ端末にて実行されているプログラムからのユーザ情報の読出手段に基づいて、当該記憶手段に記憶されているパスワードを用いて、上記管理された領域から上記ユーザ情報を読み出すステップと、を備えるユーザ使用制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯情報記憶媒体、ユーザ使用制御システム、ユーザ使用制御方法およびユーザ使用制御プログラムに係り、特に、ユーザの利便性を向上させるための発明に関する。

【0002】

【従来の技術】従来、各企業や官公庁などは、社内に所謂イントラネットを施設し、これに接続されたユーザ端末を各社員が利用することで情報を共有し、それぞれの業務の効率化などを図ってきている。

【0003】このようにイントラネットを用いた場合、たとえばデータベースなどにおいては、アクセスしてきたユーザに対してアクセスを許可しても良いか否かを判断するためにユーザ認証などの技術が一般的に用いられている。各ユーザはそのような認証が求められた場合には、パスワードなどのユーザ情報をユーザ端末から入力

【0004】そして、このようなパスワードはそのセキュリティを高めるためには、データ長が長くなり、個人が確実に覚えることができず、また、入力することができないような長さとなってしまう。そのため、銀行カード、クレジットカード、ポイントカード、プリペイドカードなどとして利用されてきたスマートカードなどの携帯情報記憶媒体を利用することが考えられる。

【0005】これにより、各ユーザは、この携帯情報記憶媒体内にユーザ情報を予め記憶させておき、これをユーザ端末に接続されたカード読取デバイスに挿入することで、情報にアクセスするために必要なユーザ情報を入力デバイスから入力することなく個人認証を行うことが可能となる。

【0006】しかしながら、このような携帯情報記憶媒体内に所定のユーザ情報を記憶させておいた場合、今後

は、その携帯情報記憶媒体から当該ユーザ情報が読み出されてしまう可能性を完全に否定することはできない。そして、携帯情報記憶媒体からユーザ情報を取得すれば、不正にアクセスすることが可能となってしまう。

【0007】そのため、従来、このような携帯情報記憶媒体を用いてユーザ端末を使用するユーザの個人認証などを行わせるユーザ使用制御システムにおいては、ユーザ情報をアクセスがパスワードにて管理されている領域に格納していた。

【0008】**【発明が解決しようとする課題】**ところで、所謂ワールドワイドウェブなどと呼ばれているインターネット技術に代表されるように、近年のコンピュータ技術およびネットワーク技術の発展には目覚ましいものがある。

【0009】そして、このようなインターネットなどのオープンネットワークを、各のインフラストラクチャの一部に取り入れることで、各企業は、自前のネットワークを施設する場合よりも、安価にネットワークを構築することができる、しかも、従来では到底不可能であった営業領域の管理なども容易に行うことができるようになる。

【0010】しかしながら、このようなオープンなネットワークを利用した場合、たとえば、インターネットへのダイヤルアップ接続、イントラネットへのファイアウォールの認証情報、データベースでの認証情報などの複数段階での認証が必要となる。

【0011】そして、携帯情報記憶媒体は、主に、上述したようにイントラネットにおけるユーザ認証のためのものとして発明してきた経緯から、数種のユーザ情報値にまとめて、あるいは、良くてもアプリケーション毎にまとめて、パスワードによって管理された領域に格納されている。

【0012】したがって、オープンなネットワークからイントラネット上のデータベースにアクセスする場合などにおいては、ダイヤルアップ接続時、イントラネットへの接続時、データベースへの接続時などの多くの段階にて何度もパスワードを入力しなければならず、使い難いなどの問題がある。

【0013】また、各アプリケーションプログラムを起動する度に、パスワードを入力しなければならず、とても使い難いなどの問題もある。

【0014】本発明は、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する度に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の利便性を逸した携帯情報記憶媒体、ユーザ使用制御システム、ユーザ使用制御方法およびユーザ使用制御プログラムを得ることを目的とする。

【0015】

【課題を解決するための手段】上記の目的のために、本発明の携帯情報記憶媒体は、ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用するユーザ情報を記憶する携帯情報記憶媒体であって、当該ユーザ情報は、パスワードを用いてアクセスできるように記録されているものである。

【0016】この構成を採用すれば、ユーザが入力したパスワードをユーザ端末において保持して再利用するだけで、複数のプログラムを利用することができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する度に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の高い利便性を提供することができる。

【0017】本発明の携帯情報記憶媒体は、ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用する複数のユーザ情報を記憶する携帯情報記憶媒体であって、当該複数のユーザ情報は、共通のパスワードにてそれぞれのユーザ情報に対してアクセスできるように記録されているものである。

【0018】この構成を採用すれば、ユーザが入力したパスワードをユーザ端末において保持して再利用するだけで、複数のプログラムにて利用する複数のユーザ情報を読み出すことができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する度に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の高い利便性を提供することができる。

【0019】本発明の携帯情報記憶媒体は、ユーザ端末に挿入され、当該ユーザ端末上で実行する複数のプログラムにて利用する複数のユーザ情報を記憶する携帯情報記憶媒体であって、当該複数のユーザ情報は、所定のパスワードによりアクセスが管理されている領域内に記録されているものである。

【0020】この構成を採用すれば、ユーザが入力したパスワードをユーザ端末において保持して再利用するだけで、複数のプログラムにて利用する複数のユーザ情報を読み出すことができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する度に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の高い利便性を提供することができる。

【0021】本発明の携帯情報記憶媒体は、各ユーザ情報は、ユーザ情報毎に固有の識別番号に対応付けられて記録されているものである。

【0022】この構成を採用すれば、ユーザは各種のユーザ端末上に共通にインストールされたプログラムにつ

いては、ユーザ端末を選ぶことなくこれを利用することができる。また、同一のユーザ端末にインストールされた複数のプログラムも、それらで共通のユーザ情報を利用することが可能となる。

【0023】本発明のユーザ使用制御システムは、ユーザ端末に組み込まれ、携帯情報記憶媒体に記憶されているユーザ情報を利用して各種のプログラムの実行および／または処理を管理するユーザ使用制御システムであって、上記プログラムからの要求に基づいて、上記いずれかの携帯情報記憶媒体から上記ユーザ情報を読み出すユーザ情報読出手段と、最初のユーザ情報の読出要求に基づいてユーザにパスワードを入力させるパスワード入力手段と、上記パスワードを記憶する記憶手段と、例えば、上記ユーザ情報読出手段は、当該記憶手段に記憶されているパスワードを用いて上記ユーザ情報を読み出すものである。

【0024】この構成を採用すれば、パスワード入力手段の要求に基づいてユーザが入力したパスワードを記憶手段に記憶させ、これを複数のプログラムにて共通に利用することができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する際に当該管理された領域にアクセスするためにパスワードを入力する必要があることなく、これによりユーザ端末の高い利便性を提供することができる。

【0025】本発明のユーザ使用制御システムは、前記プログラムからのユーザ情報読出手段を記憶手段に記憶させ、先に受け付けた要求から順番に前記ユーザ情報読出手段に受け渡す要求排他制御手段を設けたものである。

【0026】この構成を採用すれば、複数のプログラムから同時にユーザ情報の取得要求があつたとしても、ユーザ情報読出手段はこれを順番にひとつづつ確実に処理することができる。これにより、ユーザ情報の取得要求の同時発生を気にすることなく、ユーザは複数のプログラムを利用することができ、ユーザ端末の高い利便性を提供することができる。

【0027】本発明のユーザ使用制御システムは、前記ユーザ情報読出手段は、前記プログラムからのユーザ情報読出手段を、前記携帯情報記憶媒体で処理可能な要求に変換した上で当該携帯情報記憶媒体に対する読出し処理を行うものである。

【0028】この構成を採用すれば、ユーザ情報読出手段が、プログラムからのユーザ情報読出手段を、携帯情報記憶媒体で処理可能な要求に変換するので、携帯情報記憶媒体の仕様や規格を気にすることなく、各プログラムにおけるユーザ情報読出手段などをプログラミングすることができる。したがって、ユーザ情報読出手段を生成するプログラムを容易に開発することができる。

【0029】本発明のユーザ使用制御方法は、ユーザ端

末で利用する各種のユーザ情報をパスワードにてアクセスが管理された領域に格納し、当該ユーザ情報への最初のアクセスの際にユーザに上記パスワードを入力させて上記管理された領域からユーザ情報を読出し、次回からのユーザ情報へのアクセスの際には、上記パスワードを記憶しておき、これを利用して上記管理された領域からユーザ情報を読出すようにしている。

【0030】この方法を採用すれば、ユーザが入力したパスワードを記憶しておき、後から起動したプログラムにおいてもこれを利用することができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する際に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の高い利便性を提供することができる。

【0031】本発明のユーザ使用制御プログラムは、ユーザ端末にインストールされ、パスワードにてアクセスが管理された領域からユーザ端末で利用する各種のユーザ情報を読み出すユーザ使用制御プログラムであって、上記ユーザ端末にて実行されているプログラムからの最初のユーザ情報の読出要求に基づいてユーザにパスワードを入力させるステップと、上記パスワードを記憶手段に記憶させるステップと、上記ユーザ端末にて実行されているプログラムからのユーザ情報の読出要求に基づいて、当該記憶手段に記憶されているパスワードを用いて、上記管理された領域から上記ユーザ情報を読み出すステップと、を備えるものである。

【0032】この構成を採用すれば、ユーザ端末にて実行されているプログラムからの最初のユーザ情報の読出要求に基づいてユーザにパスワードを入力させ、これを複数のプログラムにて共通に利用することができる。したがって、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する際に当該管理された領域にアクセスするためにパスワードを入力する必要があることなく、これによりユーザ端末の高い利便性を提供することができる。

【0033】

【発明の実施の形態】本発明の実施の形態に係る携帯情報記憶媒体、ユーザ使用制御システム、ユーザ使用制御方法およびユーザ使用制御プログラムについて図に基づいて説明する。ユーザ使用制御方法は、ユーザ使用制御システム全体の動作として説明する。また、ユーザ使用制御プログラムなどの各種のプログラムは、一般的には、プログラムを記録したコンピュータ読取可能な記録媒体にて各使用者に提供されるものであるが、この実施の形態では、当該記録媒体に記録された上記プログラムがユーザ使用制御システムのプログラム記憶部に1に亘りインストールされているものとして説明する。

【0034】図1は、本発明の実施の形態1によるユー

サ使用制御システムの一例を示すシステム構成図である。

【0035】本発明のユーザ使用制御システムは、スマートフォンなどの携帯情報記憶媒体としてのカード型情報記憶媒体1と、このカード型情報記憶媒体1が挿入されるカード読取デバイス2を備えるユーザ端末3と、このユーザ端末3に接続されたネットワーク4と、このネットワーク4に接続され、各種のデータを保持するデータベース5、6と、を備える。

【0036】なお、これらのデータベース5、6は、たとえば、ホームページなどのオープンなデータを記憶したり、一部のユーザのみしかアクセスを許可しない営業機密情報などのクローズドなデータを記憶したりするものである。特に、クローズドなデータである場合には、ユーザ端末3からのアクセスがあった場合にそのユーザ認証を行うものである。

【0037】ネットワーク4は、オープンネットワークとしてのインターネット7と、このインターネット7にファイアウォール8を介して接続されるとともに一方のデータベース5が接続されたイントラネット9と、インターネット7にファイアウォール10を介して接続されるとともに他方のデータベース6およびユーザ端末3が接続されたイントラネット11とを、備える。そして、各ファイアウォール8、10は一般的に、インターネット7からのアクセスリクエストがあるユーザ認証などの処理を行い、適格者である場合にはインターネット7へのアクセスを許可するように構成されている。

【0038】ユーザ端末3は、主に、各種の演算処理および制御処理をプログラムに基づいて実行する中央処理装置(CPU: Central Processing Unit)12と、この中央処理装置12がプログラムの実行の際に利用するシステムメモリ13と、中央処理装置12によって設定された時間において中央処理装置12にタイム割り込みを行うタイマ14と、上記プログラムを記憶するプログラム記憶部15および当該プログラムの実行の際に利用する各種のデータを記憶するデータ記憶部(記憶手段)16を備えるストレージデバイス17と、これらを相互に接続するシステムバス18と、を備える。

【0039】このユーザ端末3においては、更に、システムバス18に、周辺機器インタフェース部(周辺機器I/F部)19が接続され、更に、この周辺機器インタフェース部19に、入力デバイス20、表示デバイス21、印刷デバイス22、通信デバイス23およびカード読取デバイス2などの各種の周辺デバイスが接続されている。なお、イントラネット11には、直接的にはこの通信デバイス23が接続されている。

【0040】図2は、図1のユーザ使用制御システム中の、カード型情報記憶媒体1の一例を示す回路ブロック図である。

【0041】カード型情報記憶媒体1は、各種の演算処理および制御処理をプログラムに基づいて実行する中央処理装置(CPU)24と、この中央処理装置24がプログラムの実行の際に利用するシステムメモリ25と、上記プログラムを記憶するプログラム記憶部26および当該プログラムの実行の際に利用する各種のデータを記憶するデータ記憶部27を備えるカードメモリ28と、これらを相互に接続するシステムバス29と、を備える。また、上記中央処理装置24には、カード挿入時にカード読取デバイス2と直接に接続されるカード1ノド部30が接続されている。なお、この実施の形態では、カード読取デバイス2に挿入される接触式のスマートカードを例に説明しているが、携帯できる情報記憶媒体であれば、非接触式のスマートカードであっても同様の利便性を備える。

【0042】プログラム記憶部26には、データ入出力制御プログラム31、規格コマンド実行プログラム32、暗号化プログラム33、その他の中央処理装置24が実行するプログラムが記憶されている。なお、このように暗号化プログラム33を当該中央処理装置24にて実行しても良いが、セキュリティ面を更に向上させる場合には、当該中央処理装置24とは別に、暗号化に特化した特異な演算ロジックによって演算処理を行う暗号処理装置を別途併設し、ここで暗号化および復号化処理を行うようにすればよい。

【0043】データ入出力制御プログラム31は、ユーザ端末3の中央処理装置12からシステムバス18、周辺機器I/F部19、カード読取デバイス2を通じてカード1ノド部30へ送付されてきたセッション確立リクエストに基づいてシステムメモリ25に読み込まれ、中央処理装置24にて実行されるものである。このデータ入出力制御プログラム31は実行する中央処理装置24は、ユーザ端末3の中央処理装置12からの規格別コマンドを受信し、更に当該規格別コマンドの実行の結果を当該中央処理装置12へ応答するものである。また、この応答の後に実行が終了され、セッションを開放する。

【0044】規格コマンド実行プログラム32は、上記規格別コマンドの受信に応じてシステムメモリ25に読み込まれ、中央処理装置24にて実行されるものである。この規格コマンド実行プログラム32を実行する中央処理装置24は、規格別コマンドを実行し、たとえばその実行によってデータ記憶部27から所定のデータを読み出す処理などを実行する。

【0045】暗号化プログラム33は、暗号化処理あるいは復号化処理をする際システムメモリ25に読み込まれ、中央処理装置24にて実行されるものである。これにより、各種のユーザ情報を暗号化してデータ記憶部27に記憶させ、更に、それを復号してユーザ端末3にて利用させることができる。

【0046】ところで、カード型情報記憶媒体1には、

単にコマンド実行プログラムではなく、規格コマンド実行プログラムと表記したように、その用途などに応じて多数の規格が存在する。たとえば、銀行がそのサービスを提供するために制定した規格、クレジット会社が自社のサービスを提供するために制定した規格、官公庁がそのサービスを提供するために制定した規格などの規格がある。また、企業やネット網におけるセキュリティを提供している会社においても、それぞれ独自の規格を制定している。このように各社はそれぞれ独自の規格を制定することで、より安全性の高いユーザ情報の管理サービスを提供することができる。

【0147】したがって、これらのサービスを利用する各種の応用A Pプログラムにおいては、通常は、規格毎に異なるコマンド（規格別コマンド）をカード型情報記憶媒体1に送信し、これにより所定のユーザ情報を取得しなければならない。

【0148】データ記憶部27には、カード識別番号34などとともに、ネットワークログイン情報35、データベースログイン情報36、クライアントログイン情報37、電子マネー情報38、ユーザ識別情報39、ユーザ端末ログイン情報40、ダイヤルアップ情報41、その他の上記ユーザ端末3などにおいて利用する各種のユーザ情報が記憶されている。

【0149】このカード識別番号34は、当該カード型情報記憶媒体1を提供するカードバンクや、当該バンク内でのカードの種類などに応じた固有の番号である。これにより、当該カード型情報記憶媒体1の種類や対応している規格を判断することができる。

【0150】図9は、図2のカード型情報記憶媒体1中の、データ記憶部27のデータマッピングの一例を示す説明図である。

【0151】データ記憶部27は、その先頭位置から設定された1つのマスターファイルの管理領域42、複数のデタキエクトファイルの管理領域43とからなる。各管理領域42、43は、それぞれ、データ記憶部27上に連続した領域にて設定されている。

【0152】マスターファイルの管理領域42には、その先頭位置にマスターファイル44（図3において管理領域42中の「MFタグ番号」で始まる「」にてくられた部分）が格納され、それに続けて1つあるいは複数個のエレメンタリファイル45（図3において管理領域42中の「EFタグ番号」で始まる「」にてくられた部分）が格納されている。

【0153】各デタキエクトファイルの管理領域43には、その先頭位置にデタキエクトファイル46（図3において管理領域43中の「DTタグ番号」で始まる「」にてくられた部分）が格納され、それに続けて1つあるいは複数個の別のタグ番号が割り当てられる。この例は上記マスターファイル44のタグ番号と異なる値とする、デタキエクトファイル

ーザ情報は、後述するように、このデタキエクトファイルの管理領域43に格納されたエレメンタリファイル47のデータフィールドに格納される。

【0154】図4を用いて、更にデータ記憶部27のデータマッピング方法について説明する。

【0155】この実施の形態では、図4（A）に示すように、データ記憶部27は、1つのマスターファイルの管理領域42と、複数のデタキエクトファイルの管理領域43とに分類して管理される。

【0156】マスターファイルの管理領域42は、データ記憶部27の先頭位置を含む領域として設定され、各デタキエクトファイルの管理領域43はそれ以外の領域をそれぞれに連続する1つのアドレス空間となるように所定のデータサイズ毎に定義される。そしてたとえば複数のユーザ端末3の全てにおいてシングルサインイン（1つのIDによってたとえばユーザ端末3内の全てのプログラムの利用を可能とすること）を実現しようとした場合には、各デタキエクトファイルの管理領域43を、当該カード型情報記憶媒体1を操作するユーザ端末3の数だけ設けられ、図4では、8つのユーザ端末3においてシングルサインインを実現することができる。

【0157】マスターファイルの管理領域42には、その先頭位置にマスターファイル（図4（A）では「MF」と表記している。）44が格納され、それに続いて各種のエレメンタリファイル（「EF」と表記）45が格納されている。各デタキエクトファイルの管理領域43には、その先頭位置にデタキエクトファイル（「DF」と表記）46が格納され、それに続いて各種のエレメンタリファイル（「EF」と表記）47が格納されている。

【0158】マスターファイル「MF」44は、図4（B）に示すように、タグフィールドと、サイズフィールドと、データフィールドとからなる。マスターファイル「MF」44のタグフィールドには、当該カード型情報記憶媒体1の規格などに基いて予め定められた特定のタグ番号が割り当てられる。マスターファイル「MF」44のデータフィールドには、たとえば、当該カード型情報記憶媒体1に設けられた全てのデタキエクトファイル「DF」46の総数（タグフィールド値）などが格納されている。サイズフィールドには、このデータフィールドのバイト数、ビット数などのサイズに応じた値が格納されている。

【0159】デタキエクトファイル「DF」46は、図4（C）に示すように、タグフィールドと、サイズフィールドと、データフィールドとからなる。デタキエクトファイル「DF」46のタグフィールドには、それぞれ固有の値に異なる値のタグ番号が割り当てられる。この例は上記マスターファイル44のタグフィールドのタグ番号とも異なる値とする、デタキエクトファイル

【DF】46のデータフィールドには、たとえば、当該データフィールドの管理領域43内のエレメンタリファイル【EF】47に対してアクセスするために必要なパスワードなどが格納されている。

【0060】エレメンタリファイル【EF】45、47は、図4(D)に示すように、タグフィールドと、サイズフィールドと、データフィールドとからなる。エレメンタリファイル【EF】45、47のタグフィールドには、それぞれに固有の互いに異なる値のタグ番号が割り当てられる。この値は上記マスターファイル44のタグ番号の値および上記データフィールド46のタグ番号の値とも異なる値とするとともに、ユーザ情報毎に固有の値とする。1つのプログラムにおいて複数のユーザ情報を利用する場合には、ユーザ情報毎に固有の値とする。

【0061】また、エレメンタリファイル【EF】45、47のデータフィールドには、それがデータフィールドの管理領域43に格納される場合には、ユーザ情報そのものがあるいは略号化されたものが格納され、マスターファイルの管理領域43に格納される場合には、カード識別番号などのカード全体を管理するためのデータがそのまゝあるいは略号化されて格納される。

【0062】このように、この実施の形態のカード型情報記憶媒体1では、各ユーザ情報やカード識別番号は、それぞれに対して固有のタグ番号が対応付けられて別々のファイル(エレメンタリファイル【EF】47)として管理されている。また、各ファイル(エレメンタリファイル【EF】47)は、1回のパスワード入力によって実行された1種類の応用Aプログラム49、50、51(図5参照)あるいはユーザ端末3毎に、且つ、1つのパスワードによってアクセス管理がされた領域(データフィールドの管理領域43)に分類されることになる。

【0063】なお、このようなデータマッピングがなされているカード型情報記憶媒体1から所定のユーザ情報を読み出すためには、基本的には、まず、中央処理装置24において、当該ユーザ情報を格納するデータフィールドの管理領域43を特定させ、次に、当該データフィールド【DF】46に格納されているパスワードを照合させ、そのパスワードが一致した上で、上記ユーザ情報を格納するエレメンタリファイル【EF】47を参照させ、更に、そのエレメンタリファイル47のデータフィールドから上記ユーザ情報を読み出させることになる。

【0064】図5は、図1のユーザ使用制御システム中の、プログラム記憶部15の構成例を示す説明図である。

【0065】このストレージデバイス17のプログラム記憶部15には、図示外の記憶媒体からインストールされたプログラムとして、オペレーティングシステムプロ

グラム(OSプログラム)48、更に、このOSプログラム48の管理の下で中央処理装置12にて実行される、通称応用アプリケーションプログラム(通称応用Aプログラム)49、クライアント応用アプリケーションプログラム(クライアント応用Aプログラム)50、電子取引応用アプリケーションプログラム(電子取引応用Aプログラム)51、シングルサインインアプリケーションプログラム(シングルサインインAプログラム)52、その他の中央処理装置12で実行するアプリケーションプログラムが記憶されている。

【0066】OSプログラム48は、システムリソース監視制御プログラム53、プログラム排他制御プログラム54、プログラム間通信プログラム55、その他のユーザ端末上で各種のアプリケーションプログラムを実行するためのプログラムからなる。

【0067】システムリソース監視制御プログラム53は、ユーザ端末3への電源投入などに応じて最初にシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。システムリソース監視制御プログラム53を実行する中央処理装置12(図6におけるシステムリソース監視制御手段56に相当)は、主に、タイム14、周辺機器デバイス20、21、22、23、2などからの割り込みを管理したり、データやコマンドをタイム14、周辺機器デバイス20、21、22、23、2との間で入出力したりするものである。

【0068】特に、システムリソース監視制御プログラム53を実行する中央処理装置12は、カード型情報記憶媒体1にアクセスする場合には、カード型情報記憶媒体1との間で毎回セッションを確立し、その上でコマンドをカード型情報記憶媒体1へ送附し、その応答データをカード型情報記憶媒体1から受領している。また、当該応答受信の後は、システムリソース監視制御プログラム53を実行する中央処理装置12は、上記セッションを開放する。このようにカード型情報記憶媒体1に対するアクセスの度にセッションを確立し且つ開放することによって、複数のアプリケーションプログラム(Aプログラム)が1つのカード型情報記憶媒体1に対して個別に且つ直接にアクセスすることが可能となる。

【0069】なお、現在、このようなカード型情報記憶媒体1に対するコマンド送付手順は、ISO7815-3などのデータ通信規格(プロトコル)において統一されている。

【0070】プログラム排他制御プログラム54は、ユーザ端末3への電源投入などに応じて最初にシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。プログラム排他制御プログラム54を実行する中央処理装置12は、主に、上記割り込みなどに応じて所定のプログラムをシステムメモリ13に読み込めるとともに、システムメモリ13上に読み込まれている複数のプログラムの間での実行スケジュールをタイムシェ

13

アラインメントで整理し、各プログラムを中央処理装置12に実行させるものである。

【0071】なお、これらシステムリソース監視制御プログラム53およびプログラム排他制御プログラム54は、中央処理装置12にて周期的に実行されるようにスケジューリングされる。

【0072】プログラム間通信プログラム55は、複数のプログラムの間でデータやコマンドの受け渡しを制御するプログラムであって、あるプログラムからデータやコマンドが出力された際に中央処理装置12にて実行

されるものである。【0073】通信応用Aプログラム49は、ユーザ情報取得プログラム57およびユーザ情報タグ番号リスト58を備えるものであり、入力デバイス20からの割り込みリクエストなどに応じてシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。この通信応用Aプログラム49を実行する中央処理装置12は、通信デバイス21を用いてネットワーク4上に所定の領域の仮想回線を確立したりする。

【0074】ユーザ情報タグ番号リスト58は、通信応用Aプログラム49にて使用する全てのユーザ情報について、ユーザ情報とエレメンタリファイル【EF】のタグ番号（以下、【EF】タグ番号という）とを対応付けたリストである。

【0075】ユーザ情報取得プログラム57は、通信応用Aプログラム49の実行に伴ったたとえばネットワーク4やデータベース5、6へのログイン認証時などにおいて通信システムメモリ13に読み込まれ、中央処理装置12に実行されるものである。ユーザ情報取得プログラム57を実行する中央処理装置12（図6におけるユーザ情報取得手段59に相当）は、通信応用Aプログラム49にて必要となったユーザ情報に対応する【EF】タグ番号をユーザ情報タグ番号リスト58から取得し、この【EF】タグ番号を指定した共通リドアクセスコマンドをプログラム間通信にシングルサインインAプログラム52へ受け渡し処理を行う。

【0076】なお、クライアント応用Aプログラム59は、データベース5、6上のデータなどを使用して各種のデータ処理などを実行するためのプログラムであり、入力デバイス20からの割り込みリクエストなどに応じてシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。また、電子取引応用Aプログラム51は、電子マネー（電子的なトークン）を用いてネットワーク4にて提供販売されている各種の商品やサービスを受けるためのプログラムであり、入力デバイス20からの割り込みリクエストなどに応じてシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。そして、これらの通信応用Aプログラム50、51においても、各種のユーザ情報をカード型情報記憶媒体1から取得するユーザ情報取得プログラム57

14

と、このユーザ情報取得プログラム57が各ユーザ情報を取得するために使用する【EF】タグ番号を記録したユーザ情報タグ番号リスト58と、を備え、これらを用いてカード型情報記憶媒体1から所定のユーザ情報を逐次読み出して利用している。

【0077】なお、各ユーザ情報タグ番号リスト58に登録される各ユーザ情報の【EF】タグ番号は、上述したようにユーザ情報毎に相互に異なる番号であり、このユーザ情報の種類毎に複数のユーザにおいて共通に設定された番号である。また、全く同一のユーザ情報を複数の応用Aプログラムにて利用しても、あるいは、同一の応用Aプログラムにおいて複数回に渡って利用してもかまわない。

【0078】シングルサインインAプログラム52は、上記各種の応用Aプログラム49、50、51からのユーザ情報の取得要求（上記【EF】タグ番号を指定した共通リドアクセスコマンドなど）を受信することでシステムメモリ13に読み込まれ、中央処理装置12に実行されるものである。また、このシングルサインインAプログラム52は、ユーザによる一度のパスワード入力によって、上記複数の応用Aプログラム49、50、51の利用を可能ならしめるために、共通コマンド排他制御プログラム60、共通コマンド変換プログラム61、パスワードキャッシュプログラム62、カード排他監視プログラム63、カード種別別プログラム64、カード識別番号タグ番号データ55、シングルサインインタグ番号データ66、規格別カード識別番号リスト67、コマンド対応テーブル68などを、備える。

【0079】規格別カード識別番号リスト67は、カード型情報記憶媒体1の種類や、そのカード型情報記憶媒体1にて実行可能な規格別コマンドの規格を判定するために、各カードベンダにそれぞれ提供されている各カード識別番号に対して、当該種類および当該規格を対応付けたリストである。これにより、カード識別番号に基づいて、カード読取デバイス2に挿入されているカード型情報記憶媒体1がどのベンダから供給されたものであるかなどを判定することができる。

【0080】カード識別番号タグ番号データ65は、上記カード識別番号に対応付けられた【EF】タグ番号のデータである。なお、このカード識別番号タグ番号は、当該サービスにおいては、カードベンダ、上記種類や規格などにかかわらず、所定の唯一の番号とする。

【0081】シングルサインインタグ番号データ66は、複数の応用Aプログラム49、50、51単位あるいは、ユーザ端末3単位での認証を行うために、これらのサービスを提供するベンダや企業が指定する【EF】タグ番号のデータである。

【0082】コマンド対応テーブル68は、各共通コマンドに対して、各規格における規格別コマンドを対応付けたテーブルである。これにより、カード型情報記憶

体の規格が特定できれば、共通コマンドに基づいて当該カード型情報記憶媒体1へ送信すべき規格別コマンドを特定することができる。

【0083】カード排他監視プログラム63は、シングルサインインAプログラム52の起動時にシステムメモリ13に読み込まれ、その後は、タイマ割り込みに応じてあるいはスレッドとして中央処理装置12にて周期的に実行されるものである。カード排他監視プログラム63を実行する中央処理装置12（図6におけるカード排他監視手段69に相当）は、たとえばカード読取デバイス2におけるカード挿入検出フラグなどを周期的に監視し、最初にカード型情報記憶媒体1の挿入を検出したら、カード種判定プログラム64への起動通知を出力する。

【0084】また、カード型情報記憶媒体1が抜かれたら、シングルサインインAプログラム52を構成する全てのプログラム60、61、62、63、64および後述する実行Aプリスト75に登録されている全ての応用Aプログラムに対して停止通知（コールバック）を通知するとともに、シングルサインインAプログラム52においてシステムメモリ13やデータ記憶部16に記憶させていた全てのデータを消去する。

【0085】これにより、たとえば複数のユーザ情報取得プログラム57、・・・、57に個別に、カード型情報記憶媒体1の排他を監視させた場合のように、システムメモリを多重的に無駄に浪費してしまうことなく、カード型情報記憶媒体1の抜き動作に応じて複数の応用Aプログラムの実行を停止させることができる。

【0086】カード種判別プログラム64は、カード排他監視プログラム63からの起動通知に応じてシステムメモリ13に読み込まれ、中央処理装置12にて実行されるものである。カード種判別プログラム64を実行する中央処理装置12（図6におけるカード種判定手段70に相当）は、カード識別番号タグ番号データ65を指定してカード型情報記憶媒体1に読取アクセスし、これに応じて取得したカード識別番号と規格別カード識別番号リスト67とを比較して、カード読取デバイス2に挿入されているカード型情報記憶媒体1の種類および規格を判定する。また、その判定結果をカード種データ71（図6参照）としてデータ記憶部16に記憶させる。

【0087】共通コマンド変換プログラム61は、ユーザ情報取得プログラム57から共通コマンドが出力されることに基づいてシステムメモリ13に読み込まれ、中央処理装置12にて実行されるものである。共通コマンド変換プログラム61を実行する中央処理装置12（図6においてはユーザ情報取得手段としての共通コマンド変換手段72に相当）は、カード種データ71を用いて共通コマンドを変換すべき規格を判定し、この規格および共通コマンドとを用いてコマンド対応テーブル68から所定の規格別コマンドを生成（抽出）するものであ

る。なお、この処理の結果としてコマンド対応テーブル68から抽出されてくる規格別コマンドは、1つのこともあれば、所定の順序で数個の規格別コマンドからなることもある。

【0088】また、共通コマンド変換プログラム61を実行する中央処理装置12は、上記抽出した規格別コマンドをプログラム横断的にシステムリソース監視制御プログラム53へ送信し、このシステムリソース監視制御プログラム53からカード型情報記憶媒体1の中央処理装置24へ送信させる。

【0089】更に、共通コマンド変換プログラム61を実行する中央処理装置12は、システムリソース監視制御プログラム53から受信したユーザ情報をそれぞれに所定の応用Aプログラム49、50、51に対して通知する。

【0090】共通コマンド排他制御プログラム60は、共通コマンド変換プログラム61とともにシステムメモリ13に読み込まれ、中央処理装置12にて実行されるものである。共通コマンド排他制御プログラム60を実行する中央処理装置12（図6における要求排他制御手段としての共通コマンド排他制御手段73に相当）は、複数のユーザ情報取得プログラム57、・・・、57からの共通コマンドを共通コマンドリスト67としてデータ記憶部16に記憶させて、先に入力された共通コマンドから実行し、当該共通コマンドの実行が完了すると次の共通コマンドを順次排他的に実行させるものである。

【0091】また、この共通コマンド排他制御プログラム60を実行する中央処理装置12は、共通コマンドを受留し且つ終了していない全ての応用Aプログラム49、50、51のリストを実行Aプリスト75としてデータ記憶部16に記憶させる。

【0092】パスワードキャッシュプログラム62は、これら共通コマンド変換プログラム61や共通コマンド排他制御プログラム60の最初の実行の際に、パスワード76（図6参照）がデータ記憶部16に格納されていないことなどに基づいてシステムメモリ13に読み込まれ、中央処理装置12にて実行されるものである。パスワードキャッシュプログラム62を実行する中央処理装置12（図6においてはパスワード入力手段としてのパスワードキャッシュ手段77に相当）は、表示デバイス21にシングルサインイン用のパスワードを入力させるウィンドウなどを表示させ、これに対して入力された文字列などを取得し、これをパスワード76としてデータ記憶部16に格納する。

【0093】ここで、コマンド対応テーブル68を用いた、共通コマンド変換プログラム61による上記共通コマンドのコマンドインタプリタ処理の意義について詳しく説明する。

【0094】上述したように、各カード型情報記憶媒体

1のペンダは、セキュリティなどを確保するためにそれぞれに独自のコマンド体系にて、データ記憶部27に対するデータの読み書きを制御できるようにしている。特に、セキュリティや認証が関係するペンダにおいては、あえて独自のコマンド体系を構築し、これにより高いセキュリティや認証を確保するようにしている。そのため、従来において、ユーザ情報取得プログラム57を頒発する場合には、そのプログラムが組み込まれる応用Aプログラムにおいて利用する全ての規格について別々にそれぞれの手順にてユーザ情報を取得するプログラムを作成しなければならなかった。つまり、1つの応用Aプログラムを複数の規格に基づくカード型情報記憶媒体1に対応させようとする場合には、ユーザ情報を取得するためのプログラムの数をその規格の数だけ開発しなければならなかった。

【0105】この問題を回避するために、この実施の形態では、コマンド対応テーブル68を設けている。また、各応用Aプログラムにおいては、ユーザ情報取得プログラム57から共通コマンドを出力させ、共通コマンド変換プログラム1においてこの共通コマンドを規格別コマンドに変換している。

【0106】これにより、各応用Aプログラムにおいては、共通コマンドにて記述されたプログラムを1つ開発するだけで、複数の規格に対応することができるので、それぞれが利用しようとしている純粋のカード型情報記憶媒体1の規格を全く意識する必要がなくなり、開発が極めて容易となる。

【0107】また、この実施の形態では更に、コマンド対応テーブル68自体の作り込みにも工夫を凝らしている。

【0108】特別な対策を講じなかった場合には、このように共通コマンドを定義し、これをコマンド対応テーブル68を用いてコマンドインタプリタ処理をしようとした場合、コマンド対応テーブル68には、共通コマンド毎に、全ての規格の数の規格別コマンドを別々に対応させなければならず、膨大なデータサイズのコマンドリストが必要となってしまう。

【0109】しかしながら、カード型情報記憶媒体1は、上記スマートカードに代表されるように、主に個人認証やセキュリティのために用いられるものであり、このような目的で各ペンダにより提供される規格別コマンドには、たとえば上述したデフォルトファイルの管理領域43にアクセスするためには、本来的には不要な規格別コマンドが採用されている場合が多い。また、それら本来的には不要な規格別コマンドは、基本的な規格別コマンドとセットにしてのみ利用されるものが多い。

【0110】つまり、カード型情報記憶媒体1における規格別コマンドには、データへアクセスするために本来的に必要となる本来的な規格別コマンド（複数の規格において共通に利用可能な規格別コマンド）のほか、そ

れぞれの規格独自の特殊な規格別コマンド（特定の規格においてしか利用できない規格別コマンド）が存在する。

【0111】この実施の形態では、このようなカード型情報記憶媒体1における規格別コマンドの特殊性に鑑み、各共通コマンドに直接に対応させる基本コマンドリストには基本的な規格別コマンドのみを対応させ、上記規格独自の特殊な規格別コマンドについては、カード種別データに基づいて適宜当該基本コマンドリストに付加コマンドセットを付加したコマンド対応テーブル68として記述している。また、規格独自の特殊な規格別コマンドを付加した規格別コマンドを生成するか、否かの判断のために、カード種別データを用いている。

【0112】これにより、特殊な規格別コマンドを含むコマンドリストと、それを含まないコマンドリストとを各規格別コマンド毎に設けた場合のコマンド対応テーブル68より、少ない種別データ量にてコマンド対応テーブル68を記述することができる。その結果、ユーザ情報取得プログラム57の開発の容易化と、コマンド対応テーブル68のデータ量の削減とを両立させることができる。

【0113】次に、このようなユーザ使用制御システムの動作について説明する。

【0114】ユーザ端末3の電源が投入されると、中央処理装置12は、システムメモリ13などが正常であることを確認した後、プログラム記憶部15に記憶されているOSプログラム48をシステムメモリ13に読み込み、これを実行する。これにより各種の周辺デバイス20、21、22、23、24は中央処理装置12によって管理された状態となる。

【0115】また、このOSプログラム48のシステムリソース監視制御プログラム53およびプログラム排他制御プログラム54は、上記初期設定時には、タイム14からの割り込みあるいは所定の時間毎に周期的に実行される。これにより、中央処理装置12は、周辺デバイス20、21、22、23、24からの割り込みリクエストや、周辺デバイス20、21、22、23、24に対するデータ入出力などを管理しつつ、各種のアプリケーションプログラムをタイムシェアリングにて実行することができる。

【0116】このようなOSプログラム48によるユーザ端末3の初期設定がなされた後に、ユーザの入力デバイス20に対する操作などに応じてたとえば、最初に、通称応用Aプログラム49に対する起動リクエストが中央処理装置12に入力されると、中央処理装置12は、当該応用Aプログラム49をプログラム記憶部15からシステムメモリ13に読み込み、これを実行する。

【0117】そして、この通称応用Aプログラム49では、ネットワークログイン情報やデータベースロギ

情報を用いてカード型情報記憶媒体 1 から取得するために、ユーザ情報取得プログラム 57 が起動される。

【0108】このユーザ情報取得プログラム 57 を実行する中央処理装置 12 は、ユーザ情報タグ番号リスト 58 を検索して、上記ネットワークログイン情報やデータベースログイン情報に対応する「EF」タグ番号を取得し、この「EF」タグ番号に対応するユーザ情報を読み出すための共通ユーザ情報読出コマンドを共通コマンド排他制御プログラム 60 にプログラム通知により受け渡す。

【0109】共通コマンド排他制御プログラム 60 を実行する中央処理装置 12 は、当該通信応用 A プログラム 49 を実行 A プリスト 75 に登録するとともに、上記共通ユーザ情報読出コマンドを共通コマンド変換プログラム 61 に受け渡す。

【0110】また、パスワードキャッシュプログラム 62 が中央処理装置 12 により実行され、その結果、ユーザが入力デバイス 20 などを使用して入力した文字列がキャッシュパスワード 76 としてデータ記憶部 16 に記憶される。なお、このデータ記憶部 16 では、上記文字列を暗号化して記憶しておくほうが好ましい。

【0111】共通コマンド変換プログラム 61 を実行する中央処理装置 12 は、カード種データ 71 およびコマンド対応テーブル 68 を用いて上記共通ユーザ情報読出コマンドをそれと等価な処理をカード型情報記憶媒体 1 の中央処理装置 24 に対して指示するための規格別コマンドを生成し、これをシステムリソース監視制御プログラム 53 に受け渡す。

【0112】ここで生成される規格別コマンドは、たとえば、シングルサインインタグ番号データ 68 を用いたディレクトリファイルの管理領域 43 を中央処理装置 24 に選択させる領域選択コマンドと、当該管理領域 43 のディレクトリファイル 46 のパスワードとキャッシュパスワード 76 を中央処理装置 24 において照合させるための照合規格別コマンドと、上記「EF」タグ番号を格納するエレメンタリファイル 41 を中央処理装置 24 に選択させるファイル選択規格別コマンドと、選択したエレメンタリファイル 41 のデータフィールドからデータを抽出させる抽出規格別コマンドと、当該読み出したデータを送還させるための送還規格別コマンドとからなる。

【0113】システムリソース監視制御プログラム 53 を実行する中央処理装置 12 は、システムバス 18 からカード 1 ノド部 30 までの経路を通じて、データ入出力制御プログラム 31 を実行するカード型情報記憶媒体 1 の中央処理装置 24 との間で FIC、C、S プロトコルなどに基づいてセッションを確立し、各規格別コマンドを送信する。また、カード型情報記憶媒体 1 の中央処理装置 24 は、各規格別コマンドを受信すると、規格コマンド実行プログラム 32 を実行する。

【0114】カード型情報記憶媒体 1 の中央処理装置 24 は、上記全ての規格別コマンドを受信し、その受信順にて順次実行する。これにより、カード型情報記憶媒体 1 では、それぞれの規格に適合した適切な規格別コマンドの処理が行われ、ユーザ端末 3 の中央処理装置 12 は、カード型情報記憶媒体 1 の種類にかかわらず、「EF」タグ番号に対応付けられたネットワークログイン情報やデータベースログイン情報を用いてカード型情報記憶媒体 1 から取得することができる。

【0115】これらのカード型情報記憶媒体 1 から取得したユーザ情報は、共通コマンド変換プログラム 61 に基づいて動作する中央処理装置 12 から、通信応用 A プログラム 49 のユーザ情報取得プログラム 57 へ受け渡され、通信応用 A プログラム 49 を実行する中央処理装置 12 は、通信デバイス 21 からネットワークログイン情報を送信することで、イントラネット 9、11 に対する仮想回線を確立したり、通信デバイス 21 からデータベースログイン情報を送信することで、データベース 5、6 上のデータを読み書きすることが可能となる。

【0116】このように通信応用 A プログラム 49 がカード型情報記憶媒体 1 にアクセスした後では、クライアント応用 A プログラム 50 がそのユーザ情報取得プログラム 57 を用いてクライアントログイン情報を取得する場合には、シングルサインイン用のパスワードがデータ記憶部 16 にキャッシュパスワード 76 として格納されているので、パスワードキャッシュプログラム 62 は起動されない。

【0117】同様に、電子取引応用 A プログラム 51 がそのユーザ情報取得プログラム 57 を用いて電子マネー情報を取得する場合には、シングルサインイン用のパスワードがデータ記憶部 16 にキャッシュパスワード 76 として格納されているので、パスワードキャッシュプログラム 62 は起動されない。

【0118】なお、共通コマンド変換プログラム 61 が動作中に、新たな共通コマンドを受信したら、共通コマンド排他制御プログラム 60 を実行する中央処理装置 12 は、この共通コマンドを共通コマンド FIF 704 に順次記憶させて、先に入力された共通コマンドの実行が終了した次の共通コマンドを順次共通コマンド変換プログラム 61 へ受け渡す処理を行う。

【0119】このように、複数の応用 A プログラム 49、50、51 で使用するユーザ情報を 1 つのパスワードで管理されたディレクトリファイルの管理領域 43 に格納し、更に、ユーザが入力したパスワードをその使用が終了するまで、データ記憶部 16 にキャッシュしておくことで、ユーザは 1 回パスワードを入力すればそれら複数の応用 A プログラム 49、50、51 を利用することができる。これにより、ユーザによってシングルサインインサービスを提供することができる。

【0120】以上の複数の応用 A プログラム 49、5

0, 51によるカード型情報記憶媒体1に対するアクセスをまとめると、図9に示すような態様となる。各応用APPプログラムからのユーザ情報抽出・要求は、同図の上側の手段から下側の手段に順番に送信され、それに対するユーザ情報の応答は同図の下側の手段から上側の手段に順番に返信される。

【0121】以上の実施の形態は、本発明の好適な実施の形態であるが、本発明の要旨を逸脱しない範囲において、種々の変更が可能である。たとえば、上記実施の形態では、ユーザ端末3としてユーザが直接に使用するものの場合について述べたが、この他にも、たとえば、クレジットカード、プリペイドカード、自動引き落としカード、電子マネーなどによる支払いを処理する店員が使用するユーザ端末や、建売物への出入り口などに設けられ、当該建売物へのユーザの出入りを管理するためのユーザ端末などにおいても好適に利用することができる。

【0122】また、この実施の形態では、当該カード型情報記憶媒体1内に設けるデディケートファイルの管理領域43を、当該記憶媒体1を挿入するユーザ端末3の数だけ設け、全てのユーザ端末3においてシングルサインインができるようにしているが、たとえば機密性の高いデータなどに対してアクセスする応用APPプログラムにて使用するユーザ情報などについては、同一のユーザ端末3上で利用されるそれ以外の応用APPプログラムがあったとしても、それとは異なるデディケートファイルの管理領域43に管理し、別なパスワードを入力させるようにしても構わない。この場合には、カード型情報記憶媒体1内に設けるデディケートファイルの管理領域43の数は、それを挿入するユーザ端末3の数よりも多くなる。逆に、複数のユーザ端末3において1つのデディケートファイルの管理領域43を利用するように設定しても良いことは言うまでもない。

【0123】更に、この実施の形態では、最初の応用APPプログラム49の起動時にユーザ使用制御プログラム57を起動させ、このタイミングにおいて当該ユーザ端末3で利用するデディケートファイルの管理領域43へアクセスするためのパスワードを入力させるようにしているが、05プログラム48の起動時に当該パスワードを入力させるようにしてもよい。この場合には、複数の応用APPプログラム49, 50, 51に対するシングルサインインサービスではなく、ユーザ端末3毎のシングルサインインサービスとなる。

【0124】また更に、この実施の形態では、携帯情報記憶媒体として、カード型情報記憶媒体1を例として説明したが、1507816にて開示されているSPOM (self-programmable on-chip microcomputer) 型のICチップなどを組み込んだ携帯電話端末であっても、その他の小型のリムーバブルなメモリデバイスなども同様に応用することができる。

【0125】

【発明の効果】以上のように、本発明では、ユーザ情報をパスワードで管理された領域で管理して高いセキュリティを確保しながらも、ユーザ端末上でプログラムを使用する際に当該管理された領域にアクセスするためにパスワードを入力する必要がなく、これによりユーザ端末の利便性を追求した携帯情報記憶媒体、ユーザ使用制御システム、ユーザ使用制御方法およびユーザ使用制御プログラムを得ることができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1によるユーザ使用制御システムの一側を示すシステム構成図である。

【図2】 図1のユーザ使用制御システム中の、カード型情報記憶媒体の一側を示す回路ブロック図である。

【図3】 図2のカード型情報記憶媒体中の、データ記憶部のデータマッピングの一側を示す説明図である。

【図4】 図3に示すデータ記憶部におけるデータマッピング方法の説明図である。

【図5】 図1のユーザ使用制御システム中の、プログラム記憶部の構成図を示す説明図である。

【図6】 図1のユーザ使用制御システムにおいて、複数の応用APPプログラムによるカード型情報記憶媒体に対するアクセスを示す概念図である。

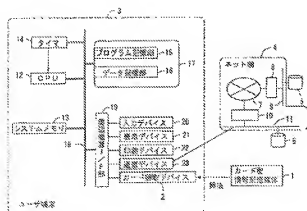
【符号の説明】

- 1 カード型情報記憶媒体 (携帯情報記憶媒体)
- 2 カード読取デバイス
- 3 ユーザ端末
- 4 ネット網
- 5, 6 データベース
- 7 インターネット
- 8, 10 ファイアウォール
- 9, 11 イントラネット
- 12 中央処理装置 (CPU)
- 13 システムメモリ
- 14 タイマ
- 15 プログラム記憶部
- 16 データ記憶部 (記憶手段)
- 17 ストレージデバイス
- 18 システムバス
- 19 周辺機器インタフェース部 (周辺機器1/F部)
- 20 入力デバイス
- 21 表示デバイス
- 22 印刷デバイス
- 23 通信デバイス
- 24 中央処理装置 (CPU)
- 25 システムメモリ
- 26 プログラム記憶部
- 27 データ記憶部
- 28 カードメモリ
- 29 システムバス

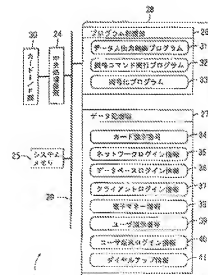
- 30 カードI/F部
 31 データ入出力制御プログラム
 32 規格コマンド実行プログラム
 33 暗号化プログラム
 34 カード識別番号
 35 ネットワークログイン情報
 36 データベースログイン情報
 37 クライアントログイン情報
 38 電子マネー情報
 39 ユーザ識別情報
 40 ユーザ端末ログイン情報
 41 ダイアルアップ情報
 42 マスターファイルの管理領域
 43 デディケートファイルの管理領域
 44 マスターファイル
 45、47 エレメンタリファイル
 46 デディケートファイル
 48 オペレーティングシステムプログラム (OSプログラム)
 49 通信応用アプリケーションプログラム (通信応用
 APプログラム)
 50 クライアント応用アプリケーションプログラム
 (クライアント応用APプログラム)
 51 電子取引応用アプリケーションプログラム (電子
 取引応用APプログラム)
 52 シングルサインインアプリケーションプログラム*

- * (シングルサインインAPプログラム)
 53 システムリソース監視制御プログラム
 54 プログラム排他制御プログラム
 55 プログラム間通信プログラム
 56 システムリソース監視制御手段
 57 ユーザ情報取得プログラム
 58 ユーザ情報タグ番号リスト
 60 共通コマンド排他制御プログラム
 61 共通コマンド変換プログラム
 62 パスワードキャッシュプログラム
 63 カード接続監視プログラム
 64 カード種別プログラム
 65 カード識別番号タグ番号データ
 66 シングルサインインタグ番号データ
 67 規格別カード識別番号リスト
 68 コマンド対応テーブル
 69 カード接続監視手段
 70 カード種別手段
 71 カード種データ
 72 共通コマンド変換手段 (ユーザ情報取出手段)
 73 共通コマンド排他制御手段 (要求排他制御手段)
 74 共通コマンドI/F
 75 実行APリスト
 76 キャッシュパスワード
 77 パスワードキャッシュ手段 (パスワード入力手
 段)

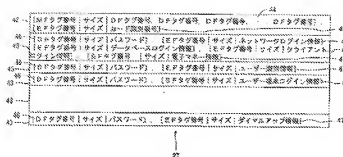
【図1】



【図2】



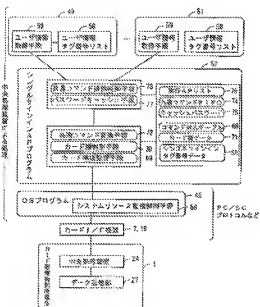
【図3】



【図5】



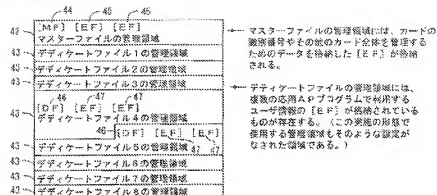
【図6】



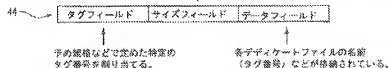
【図4】

データ記憶部のデータマッピング方法

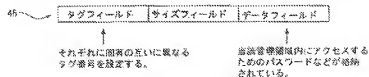
(A) データマッピング



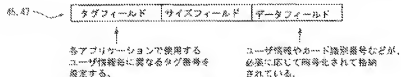
- (B) マスターファイル [MF] の構造 注1. データ記憶領域の先頭位置に記憶される。
 データフィールドのサイズに応じた値が格納される。



- (C) デリケートファイル [DF] の構造 注1. 各デリケートファイルはそれぞれの管理領域の先頭位置に記憶する。



- (D) エレメンタリファイル [EF] の構造 注1 ユーザ情報毎や管理データ毎に設ける。
 注2 ユーザ情報用のエレメンタリファイルは、ユーザ識別番号に準じて、1つのデリケートファイルの管理領域内に記憶する。



- (E) 全てのタグ番号は、少なくとも各カード型情報記憶部において、互いに異なる値となるように設定する。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-084849

(43)Date of publication of application : 19.03.2003

(51)Int.Cl.

G06F 1/00

(21)Application number : 2001-275942

(71)Applicant : NEC GUMMA LTD

(22)Date of filing : 12.09.2001

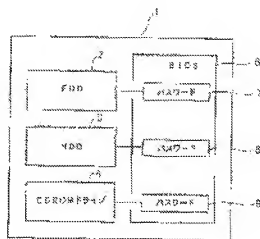
(72)Inventor : SUNAGA TAKESHI

(54) STARTING CONTROL METHOD FOR COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a starting control method for a computer capable of preventing starting of a CDROM which destroys system data.

SOLUTION: If a startable CDROM which destroys the system data with starting of the computer is inserted in a CDROM drive 4, input request for the name of a starting drive and a password is shown to a user before a starting flow begins, and it is warned that the startable CDROM exists in the CDROM drive 4. Thus, the system data is prevented from being destroyed in case the CDROM which destroys the system data.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-143443

(43)Date of publication of application : 29.05.1998

(51)Int.Cl.

G06F 12/14

G06F 3/06

G06F 13/10

(21)Application number : 08-305016

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 15.11.1996

(72)Inventor : MAEDA MAYUMI

(54) COMPUTER SYSTEM AND HARD DISK PASSWORD CONTROL METHOD FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide optimum hard disk drive(HDD) password check processing in a system loaded with plural HDD.

SOLUTION: When an HDD 14 of 1st priority is turned to access enable state by an HDD password check, a power-on self-test(POST) to be first executed by a CPU 11 at the power-on time of system executes a boot strap regardlessly of the state of an HDD 15 of 2nd-priority.

Therefore, a user can utilize a computer only by knowing an irreducibly minimum password, namely, the password of the HDD 14 to be used as a boot device. Besides, when the regular password is inputted, even concerning the HDD 15 of 2nd priority, its data can be read out or updated as well.

